NETGEAR®

User Manual

AC2000 802.11ac
Wireless Access Point/Router

Model WAC124

Support

Thank you for purchasing this NETGEAR product. You can visit
https://www.netgear.com/support/ to register your product, get help, access the latest
downloads and user manuals, and join our community. We recommend that you use
only official NETGEAR support resources.

Compliance and Conformity

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.

Do not use this device outdoors. If you connect cables or devices that are outdoors to
this device, see http://kb.netgear.com/000057103 for safety and warranty information.

Trademarks

Revision History

Publication Part Number	Publish Date	Comments
202-11885-02	December 2018	First publication.

Contents

Chapter 8 Maintain and Monitor the Access Point/Router

Chapter 11 Router Mode: Manage Dynamic DNS and FTP Access Through the Internet

Chapter 12 Router Mode: Set up VPN Connections with OpenVPN

Chapter 13 Manage the Advanced WiFi and Radio Features

Chapter 14 Router Mode: Manage Port Forwarding and Port Triggering

Chapter 15 Diagnostics and Troubleshooting

1
Hardware Overview of the Access Point/Router

The NETGEAR AC2000 802.11ac Wireless Access Point/Router Model WAC124, in this manual referred to as the access point/router, supports dual-band concurrent operation at 2.4 GHz and 5 GHz with combined throughput of 2000 Mbps (300 Mbps at 2.4 GHz and 1700 Mbps at 5 GHz). The access point/router is designed to function in a small office network or home network.

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

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/router label

Important: By default, the access point/router is in access point mode with its DHCP client enabled and must get an IP address from another router in your network. For the initial log-in process, also called single sign-on (SSO), the access point/router must connect to the Internet and you must log in with a MyNETGEAR account. (You can create an account during the log-in process.) After you complete the initial log-in process, you can change the mode to router mode and also change the settings offline.

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 four status LEDs are located on the top panel of the access point/router. From left to right, the top panel contains the Power LED, Internet LED, WiFi LED, and USB LED.

Figure 1. Top panel with LEDs

Table 1. LED descriptions

LED	Description
Power	**Solid green**. The access point/router is ready.
	Solid green temporarily, blinking green temporarily, and finally solid green. The access point/router is starting or was reset to factory default settings and is restarting. For more information about resetting the access point/router to factory default settings, see Return the access point/router to its factory default settings on page 138.
	Blinking green. The access point/router is starting or upgrading firmware. If the Power LED is blinking green at any other time, see Power LED stays blinking green on page 243.
	Off. Power is not supplied to the access point/router.
Internet	**Solid green or blinking green**. An Internet connection is established.
	Off. No Internet connection is established. For more information, see Access point mode: Internet LED is off on page 244 (access point mode is the default system mode) or Router mode: Internet LED is off on page 244.

Table 1. LED descriptions (Continued)

LED	Description
WiFi	**Solid green**. One or both WiFi radios are operating. **Blinking green**. One or both WiFi radios are sending or receiving traffic. **Blinking green slowly**. Someone pressed the **WPS** button. **Off**. Both WiFi radios are off. For more information, see WiFi LED Is Off on page 245.
USB	**Solid green**. A USB device is connected and is ready. **Off**. No USB device is connected.

Back panel with ports, buttons, and a power connector

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

Figure 2. Access point/router back panel

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

- **USB 2.0 port**. One USB 2.0 port to connect a storage device or printer to the access point/router.

- **LAN ports 4 through 1**. Four Gigabit Ethernet RJ-45 LAN ports numbered LAN4 through LAN1 to connect the access point/router to Ethernet devices such as a computer and a switch.

- **Internet port**. One Internet (WAN) port to connect the access point/router to a router, network switch, or network hub in your network (see Connect the access point/router to your existing router and log in for the first time on page 17). This port must provide the Internet connection to the access point/router.
  If you want to use the access point/router in router mode, do not connect this port to an Internet modem until after you complete the initial log-in process (see Use the access point/router in router mode on page 23).

- **WPS button**. Press the **WPS** button to join the access point/router's WiFi network without typing the WiFi password. For more information, see Use WPS to add a device to the WiFi network on page 70.

- **Reset button**. Press the **Reset** button to reset the access point/router to factory default settings. For more information, see Use the Reset button on page 138.

- **Power On/Off button**. Press the **Power On/Off** button to provide power to the access point/router.

- **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/router 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/router label

The access point/router label on the bottom panel of the access point/router shows the default login information, default WiFi network name (SSID), default WiFi passphrase, serial number and MAC address of the access point/router, and other information.
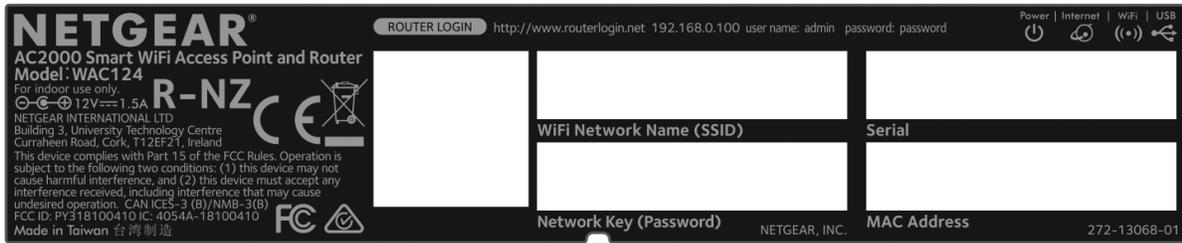
Figure 3. Access point/router label

2

Install and Access the Access Point/Router in Your Network

This chapter describes how you can install and access the access point/router in your network and go through the initial log-in process, also referred to as single sign-on (SSO). By default, the access point/router is in access point mode. You can also change the mode to router mode.

The chapter contains the following sections:

- Connect the access point/router to your existing router and log in for the first time
- Update the access point/router firmware if you cannot complete the initial log-in process
- About router mode
- Use the access point/router in router mode
- Log in to the access point/router when it is connected to the Internet
- Log in to the access point/router when it is not connected to the Internet
- Use the NETGEAR Insight mobile app to discover the access point/router
- Find the IP address of the access point/router
- Change the language
- Change the local login admin password
- Set up password recovery for the local login admin user name
- Connect a wired or WiFi device to the access point/router's network after installation

Connect the access point/router to your existing router and log in for the first time

By default, the access point/router is in access point mode and functions as a WiFi access point and LAN switch for Internet access. Basically, in access point mode, the access point/router functions as a bridge between your existing router and the access point/router's LAN and WiFi clients. The access point/router, LAN clients, and WiFi clients receive an IP address from or through your existing router.

Note: For the initial log-in process, do *not* directly connect the access point/router to an Internet modem.

For the initial log-in process, also referred to as single sign-on (SSO), the following are required:

- The access point/router must be in its default access point mode.
- The access point/router must be connected to the Internet through an existing router in your network.
- You must log in with a MyNETGEAR account. If you do not have a MyNETGEAR account, you must create one during the initial log-in process.

If you want, after you complete the initial log-in process, you can change the mode to router mode and connect the access point/router to an Internet modem (see Use the access point/router in router mode on page 23). Certain features are supported only in router mode, for example, routing services such as NAT and the DHCP server.

The easiest way to set up and start using the access point/router is to connect it to your router, 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/router to a switch or hub that is connected to the DHCP server.
When you log in to the access point/router, you connect to the local browser–based management interface, in this manual referred to as the local browser interface.

Figure 4. Connect the access point/router to another router in your network

To connect the access point/router to a router and log in to the local browser interface for the first time:

1. Connect an Ethernet cable to the yellow Internet (WAN) port on the access point/router.

2. Connect the other end of the cable to a LAN port on your router (or switch or hub that is connected to a DHCP server).

3. Power on the access point/router and check to see that the LEDs light.

LED		Description
Power		The Power LED lights solid green, then blinks green, and then lights solid green again when the startup procedure is finished. This process takes about 90 seconds. If the Power LED does not light at all, press the **Power On/Off** button on the back panel.
Internet		The Internet LED blinks green or lights solid green when the Internet connection is established.
WiFi		The WiFi LED lights solid green.

Important: Be sure that the access point/router is connected to the Internet before you continue. (The Internet LED must blink green or light solid green.)

4. Log in to the access point/router 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/router's WiFi network.
        The default SSID is NETGEAR-1. The default passphrase is **sharedsecret**.

- **Connect over Ethernet to the same network**. Using an Ethernet cable, connect the LAN port on your computer to the same router that the access point/router is connected to. You can connect your computer either directly or through a switch or hub to the router.

- **Connect over Ethernet directly to the access point/router**. Using an Ethernet cable, connect the LAN port on your computer directly to any of the four LANs port on the access point/router.

5. Launch a web browser and enter **http://www.routerlogin.net** in the address field. The Sign-In page displays.

   Note: If the Sign-In page does not display, see <u>Access point mode: You cannot log in to the access point/router</u> on page 245.

6. If the Sign-In page displays the **! A new firmware upgrade is available. Click here to get it.** button, do the following:

   a. Click the **! A new firmware upgrade is available. Click here to get it.** button. The access point/router finds the new firmware information and displays a message asking if you want to download and install it.

   b. Click the **Yes** button.
   The access point/router locates and downloads the firmware and begins the update.
   The Firmware Upgrade Assistant page displays while the firmware of the access point/router is being updated. During the update, do not turn off the power or press the **Reset** button. The update process takes about three minutes, after which the access point/router restarts.

   c. If the Sign-In page does not display, launch a web browser and enter **http://www.routerlogin.net** in the address field.

7. Depending on whether you already own a MyNETGEAR account, do *one* of the following:

   - **You already own a MyNETGEAR account**. Do the following:

     a. Click the **Login** button.
        The NETGEAR Account Login page displays.

     b. Enter your registered email address and password and click the **LOG IN** button.

- **You do not yet own a free MyNETGEAR account**. Do the following:

  a. Click the **Create** button.
     The Create NETGEAR Account page displays.

  b. Set up a new account.

  c. Log in with your MyNETGEAR registered email address and password.

Note: If the NETGEAR Account Login page or Create NETGEAR Account page does not display, if you cannot sign in to your existing MyNETGEAR account or create a new MyNETGEAR account, or if you encounter any other problem that prevents you from completing the initial log-in process, you first might need to reset the access point/router to factory default settings and then update the firmware (see Update the access point/router firmware if you cannot complete the initial log-in process on page 21. After you do so, if you still encounter problems, see Troubleshoot Internet browsing on page 251.

After you successfully log in to your MyNETGEAR account, the access point/router is registered with NETGEAR.

The BASIC Home page of the access point/router displays. You can now change the settings of the access point/router.

If new firmware is available, the BASIC Home page displays the **! A new firmware update available, Click here to get it.** button. For information about how to update the firmware, see Step 9.

8. Whether or not new firmware is available, do the following:

   a. Select **ADVANCED**.
      The ADVANCED Home page of the access point/router displays. The LAN Port pane shows the IP address that is now assigned to the access point/router.

   b. Write down the LAN IP address of the access point/router for later use.
      You must use this IP address if you plan to connect to the same network as the access point/router but not directly to the access point/router network. If you are directly connected to the access point/router network, you can use **http://www.routerlogin.net**.

9. If new firmware is available, do the following to update the firmware:

   a. Select **BASIC**.
      The BASIC Home page displays again.

   b. Click the **! A new firmware upgrade is available. Click here to get it.** button.
      The access point/router finds the new firmware information and displays a message asking if you want to download and install it.

---

c. Click the **Yes** button.
    The access point/router locates and downloads the firmware and begins the update.
    The Firmware Upgrade Assistant page displays while the firmware of the access point/router is being updated. During the update, do not turn off the power or press the **Reset** button. The update process takes about three minutes, after which the access point/router restarts. You can log in again, using your registered email address and password.

Update the access point/router firmware if you cannot complete the initial log-in process

During the initial log-in process, if the NETGEAR Account Login page or Create NETGEAR Account page does not display, if you cannot sign in to your existing MyNETGEAR account or create a new MyNETGEAR account, or if you encounter any other problem that prevents you from completing the initial log-in process, you first might need to reset the access point/router to factory default settings. Then, without logging in to your existing MyNETGEAR account or creating a new MyNETGEAR account, you can update the access point/router firmware (if new firmware is available).

After you update the firmware, you can log in to your existing MyNETGEAR account or create a new MyNETGEAR account and complete the initial log-in process.

To reset the access point/router to factory default settings and update the firmware if you cannot complete the initial log-in process:

1. Be sure that the access point/router is still connected to the Internet.

    Note: If you did not change the connection setup of the access point/router as described in Step 1 through Step 4 of Connect the access point/router to your existing router and log in for the first time on page 17, the access point/router is still connected to the Internet.

2. Reset the access point/router to factory default settings by doing the following:

    a. On the back of the access point/router, locate the **Reset** button.

    b. Using a straightened paper clip, press and hold the recessed **Reset** button until the Power LED lights yellow, which takes about five seconds.

    c. Release the **Reset** button.

The Power LED starts blinking yellow and the configuration is reset to factory default settings. When the reset is complete, the access point/router reboots and connects to the NETGEAR server to detect if new firmware is available. The entire process of resetting, rebooting, and detecting firmware takes about three minutes.

Caution: After the access point/router reboots, wait at least one more minute. If you log in too early, the access point/router might not yet have completed the firmware detection process.

3. Launch a web browser and enter **http://www.routerlogin.net** in the address field. The Sign-In page displays.

4. If the Sign-In page now displays the **! A new firmware upgrade is available. Click here to get it.** button, do the following:

    a. Click the **! A new firmware upgrade is available. Click here to get it.** button. The access point/router finds the new firmware information and displays a message asking if you want to download and install it.

    b. Click the **Yes** button.
    The access point/router locates and downloads the firmware and begins the update.
    The Firmware Upgrade Assistant page displays while the firmware of the access point/router is being updated. During the update, do not turn off the power or press the **Reset** button. The update process takes about three minutes, after which the access point/router restarts.

    c. If the Sign-In page does not display, launch a web browser and enter **http://www.routerlogin.net** in the address field.

5. Continue with of and complete the initial log-in process.

About router mode

By default, the access point/router is in access point mode and functions as a WiFi access point and LAN switch for Internet access. After initial log-in, you can change the mode of the access point/router to router mode, connect the access point/router directly to an Internet modem such as a cable or DSL modem, and log back in to the access point/router.

Important: Only after you complete the initial log-in process in access point mode (see Connect the access point/router to your existing router and log in for the first time on page 17), can you change the system mode to router mode and connect the access point/router to an Internet modem.

The following features are supported in router mode (and are 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.

- 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.

- Remote management.

- Advanced USB settings.

- Internet traffic meter.

- VLAN or bridge tag group for an IPVT device.

Note: If the access point/router is in router mode, you can always reach the local browser interface by entering **http://www.routerlogin.net** in the address field of your browser.

For information about changing the system mode of the access point/router from access point mode to router mode, see Use the access point/router in router mode on page 23 or, after initial setup, Change the system mode to router mode or back to access point mode on page 163.

Use the access point/router in router mode

When you set up the access point/router in router mode, the following applies:

- If the WAN type of your Internet modem is dynamic DHCP, the access point/router automatically receives an IP address from your Internet service provider (ISP).

- If the WAN type is PPPoE, L2TP, or PPTP, you must manually set up the Internet connection.

Note: If you are not sure what the WAN type of your modem is, contact your ISP before you start the following procedure.

Figure 5. Connect the access point/router in router mode to your Internet modem

To change to router mode, connect the access point/router directly to an Internet modem, and log back in to the local browser interface:

1. If you did not do so yet, follow the steps in <u>Connect the access point/router to your existing router and log in for the first time</u> on page 17.

   Note: Only after you complete the initial log-in process in access point mode, can you change the mode to router mode and connect the access point/router to an Internet modem.

   The BASIC Home page displays.

2. Select **ADVANCED > Advanced Setup > Wireless Access Point**.

   The Wireless Access Point page displays.

3. Clear the **Enable Access Point Mode** check box.

4. Click the **Apply** button.

   Your settings are saved and the access point/router restarts in router mode.

5. Unplug your Internet modem's power, leaving the modem connected to the wall jack for your Internet service.

   If the modem uses a battery backup, remove the battery.

6. Disconnect the Ethernet cable that is connected to the yellow Internet port of the router and connect it directly to your modem.

7. If the modem uses a battery backup, put the battery back in.

8. Plug in and turn on the modem.

9. Log in to the access point/router 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/router's WiFi network.
    The default SSID is NETGEAR-1. The default passphrase is **sharedsecret**.

    • **Connect over Ethernet directly to the access point/router**. Using an Ethernet cable, connect the LAN port on your computer directly to any of the four LANs port on the access point/router.

10. Depending on how the access point/router receives a WAN IP address, log back in to the router by doing the following:

    • **The WAN type of the modem is dynamic DHCP**. If the access point/router can connect to the Internet, the access point/router automatically receives an IP address through the modem. The Internet LED lights solid green when the access point/router is connected to the Internet. Do the following:

        a. Launch a web browser and enter **http://www.routerlogin.net** in the address field.
        The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

        b. Click the **Login** button.
        The NETGEAR Account Login page displays.

        c. Enter your registered email address and password and click the **LOG IN** button.
        The BASIC Home page displays. You can now change the router settings and other settings of the access point/router.

    • **The WAN type of the modem is PPPoE, L2TP, or PPTP**. The router cannot automatically connect to the Internet and receive an IP address through the modem. Do the following:

        a. Launch a web browser and enter **http://www.routerlogin.net** in the address field.
        The Sign-In page displays. You are prompted to sign in with the local login credentials.

        b. If you did not yet change the default password, enter **admin** as the user name and **password** as the password.
        The user name and password are case-sensitive.

        c. Click the **Login** button.
        The BASIC Home page displays.

d. Select **ADVANCED > Setup Wizard**.
    The Setup Wizard page displays.

e. Click the **Next** button.

f. During the Internet connection setup process, follow the prompts and provide the required PPPoE, L2TP, or PPTP information.
    The Internet LED lights solid green when the access point/router is connected to the Internet.

g. When you are prompted, change your admin password for local login and set up password recovery.
    The BASIC Home page displays. You can now change the router settings and other settings of the access point/router.

11. Clear the cache of your browser.

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

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

    - Router mode: You cannot log in to the access point/router on page 247

    - Router mode: Manually set up the access point/router Internet connection on page 40

    - Router mode: You cannot access the Internet on page 248

    - Troubleshoot Internet browsing on page 251

Log in to the access point/router when it is connected to the Internet

After you connected to the access point/router and logged in for the first time (see Connect the access point/router to your existing router and log in for the first time on page 17), you can log in again.

If the access point/router is connected to the Internet, you must use the registered email address and password for your NETGEAR account.

Note: You can log in even if the access point/router is not connected to the Internet. In such as situation, you must use the local login admin user name and default password (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

To log in to the access point/router when it is connected to the Internet:

1. Open a web browser from a computer or mobile device that is connected either directly to the access point/router network or to the same network as the access point/router.

   A direct connection to the access point/router 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/router.

   • **Ethernet**. A connection from a computer over an Ethernet cable to one of the LAN ports on the access point/router, either with or without a switch or hub between the computer and the access point/router.

2. Do one of the following:

   • **Directly connected**. Enter **http://www.routerlogin.net** in the address field.

   • **Connected to the same network but not directly connected**. Enter the IP address that was assigned to the access point/router by your existing router during the setup process. If you do no know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page of the local browser interface displays. You can now change the settings of the access point/router.

   The BASIC Home page displays a dashboard that lets you see the status of your access point/router at a glance.

Log in to the access point/router when it is not connected to the Internet

After you connected to the access point/router and logged in for the first time (see Connect the access point/router to your existing router and log in for the first time on page 17), you can log in again, even if the access point/router is not connected to the Internet. In such a situation, use the local login admin user name and default password, which are different from the registered email address and password for your NETGEAR account.

Note: Use the registered email address and password for your NETGEAR account only when the access point/router is connected to the Internet (see Log in to the access point/router when it is connected to the Internet on page 26).

To log in to the access point/router when it is _not_ connected to the Internet:

1. Open a web browser from a computer or mobile device that is connected either directly to the access point/router network or to the same network as the access point/router.

   A direct connection to the access point/router 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/router.

   • **Ethernet**. A connection from a computer over an Ethernet cable to one of the LAN ports on the access point/router, either with or without a switch or hub between the computer and the access point/router.

2. Enter the IP address that was assigned to the access point/router by your existing router during the setup process.

   If you do no know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. Because the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials.

3. If you did not yet change the default password, enter **admin** as the user name and **password** as the password.

   The user name and password are case-sensitive.

   For information about how to change the password for local login, see Change the local login admin password on page 32.

4. Click the **Login** button.

    The BASIC Home page of the local browser interface displays. You can now change the settings of the access point/router.

    The BASIC Home page displays a dashboard that lets you see the status of your access point/router at a glance.

Use the NETGEAR Insight mobile app to discover the access point/router

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

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

To use the NETGEAR Insight mobile app to discover the access point/router 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/router WiFi network.

3. Open the NETGEAR Insight mobile app.

4. Select **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/router displays in the device list.

5. Write down the IP address for future use.

Find the IP address of the access point/router

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

*   Your computer or mobile device is not directly connected to the access point/router network but to the same network as the access point/router.

- Your computer or mobile device *is* directly connected to the access point/router, but the access point/router is not connected to the Internet.

- 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/router or you might log in to the other NETGEAR device, depending on your network situation.

In these situations, to log in to the local browser interface of the access point/router, use the IP address that was assigned to the access point/router by your existing router during the setup process (see Connect the access point/router to your existing router and log in for the first time on page 17).

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

- Only if the access point/router is connected to the Internet, do one of the following:

  - **Option 1. Temporarily connect directly and log in**. Temporarily connect a computer or mobile device directly through an Ethernet cable or over WiFi to the access point/router and do the following:

    1. Open a web browser from a computer or mobile device that is directly connected to the access point/router 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 **LOG IN** 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/router.

  - **Option 2. Temporarily connect directly and ping the access point/router.**
    Temporarily connect a computer or mobile device directly through an Ethernet cable or over WiFi to the access point/router 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/router.

- Regardless of whether the access point/router 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/router 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/router WiFi network.

    3. Open the NETGEAR Insight mobile app.

    4. Select **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/router displays in the device list.

  - **Option 2. Access your existing router**. Access the DHCP server information of your existing router to see the devices that are connected to it, including the access point/router. The IP address that is assigned to the access point/router 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/router.

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

Change the language

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

To change the language:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
The BASIC Home page displays.

5. In the upper right corner, select a language from the menu.
The page refreshes with the language that you selected.

Change the local login admin password

We recommend that you change the default password that you use for local login to the access point/router to a more secure password. This is the password that you use to log in locally to the access point/router with the user name admin if the access point/router is not connected to the Internet.

The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

To change the password for the user name admin for local login to the access point/router:

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

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

If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

    The BASIC Home page displays.

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

    The Set Password page displays.

6. Enter the old password.

7. Enter the new password twice.

    For information about password recovery, see Set up password recovery for the local login admin user name on page 33.

8. Click the **Apply** button.

    Your settings are saved.

Set up password recovery for the local login admin user name

If you change the password for the user name admin, we recommend that you enable password recovery. This is the password that you use to log in locally to the access point/router with the user name admin if the access point/router is not connected to the Internet. Then you can recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

To set up password recovery for the local login admin user name:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Administration > Set Password**.
   The Set Password page displays.

6. Select the **Enable Password Recovery** check box.

7. Select two security questions and provide answers to them.

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

Connect a wired or WiFi device to the access point/router's network after installation

After you install the access point/router in your network (see Connect the access point/router to your existing router and log in for the first time on page 17), you can connect a device to the access point/router's LAN through an Ethernet cable or to the access point/router'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/router.

Note: Connecting to the access point/router's network is not the same as connecting to the local browser interface to view or manage the access point/router's settings. For information about logging in to the access point/router local browser interface, see Log in to the access point/router when it is connected to the Internet on page 26 or Log in to the access point/router when it is not connected to the Internet on page 28.

Connect to the access point/router through an Ethernet cable

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

For information about logging in to the access point/router local browser interface, see Log in to the access point/router when it is connected to the Internet on page 26or Log in to the access point/router when it is connected to the Internet on page 26.

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

1. Make sure that the access point/router 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/router.

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

   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/router.

   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 of the access point/router

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/router.

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 gets the security settings from the access point/router 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/router:

1. Make sure that the access point/router 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 of the access point/router for three seconds.

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/router.

Manually join the WiFi network of the access point/router

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

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

To connect a device manually to the WiFi network of the access point/router:

1. Make sure that the access point/router 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 that you want to connect to your access point/router, open the software application that manages your WiFi connections.

   This applicaiton scans for all WiFi networks in your area.

3. Look for the access point/router's network and select it.

   The default SSID is NETGEAR-1. (By default, the access point/router's second and third WiFi network are disabled.)

4. Enter the default passphrase for WiFi access.

   The default passphrase is **sharedsecret**.

5. Click the **Connect** button.

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

3
Specify the Access Point/Router Internet Settings Manually

Usually, the quickest way to set up the Internet connection is to allow the NETGEAR installation assistant to detect the Internet connection when you first set up and access the access point/router with a web browser. After initial setup, you can use the Setup Wizard at any time.

If the access point/router is in access point mode, you can specify the LAN IP settings manually.

If the access point/router 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/router is in router mode, see Router mode: Manage the LAN IP address settings on page 112.

This chapter contains the following sections:

- Use the Internet Setup Wizard
- Access point mode: Specify a fixed LAN IP address
- Router mode: Manually set up the access point/router Internet connection
- Router mode: Specify an IPv6 Internet connection

Use the Internet Setup Wizard

You can use the Setup Wizard to detect your Internet settings and automatically set up your access point/router. Although the functionality is similar, the Setup Wizard is not the same as the NETGEAR installation assistant that runs the first time that you connect to your access point/router to set it up.

The Setup Wizard can function regardless whether the access point/router is in access point mode or in router mode. In access point mode, the Setup Wizard can detect the LAN IP address that is issued by the existing router in the network. In router mode, the Setup Wizard can detect the WAN IP address that is issued by the Internet service provider.

To use the Setup Wizard:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Setup Wizard**.

   The Setup Wizard page displays.

6. Select the **Yes** radio button.

   If you select the **No** radio button, you are taken to the WAN Setup page (see <u>Router mode: Manually set up the access point/router Internet connection</u> on page 40) when you click the **Next** button.

7. Click the **Next** button.

The Setup Wizard searches your Internet connection for servers and protocols to determine your Internet configuration. When the access point/router connects to the Internet, you are prompted to change the admin password.

Access point mode: Specify a fixed LAN IP address

If the access point/router is in access point mode, you can specify the LAN IP address for the access point/router. This is the IP address of the access point/router in your existing network. If you specify a static (fixed) IP address, make sure that it is part of the LAN subnet of the existing router that assigns the LAN IP address to the access point/router.

To view the LAN settings or specify a LAN Internet connection that uses a fixed LAN IP address:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > IP Settings**.
   The IP Settings page displays.

   By default, the **Get dynamically from existing router** radio button is selected.

6. To specify a static (fixed) IP address for the access point/router, do the following:

   a. Select the **Use fixed IP Address (not recommended)** radio button.
      The fields become available.

   b. Enter the static IP address, IP subnet mask, and gateway IP address.
      These IP addresses must be in the LAN subnet of your existing router.

   c. Enter the IP address of your network's primary DNS server. If a secondary DNS
      server address is available, enter it also.

7. Click the **Apply** button.

   Your settings are saved. The access point/router restarts with the new IP address.
   To log back in to the access point/router, use the new IP address.

Router mode: Manually set up the access point/router Internet connection

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

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

Router mode: Specify a dynamic or fixed WAN IP address Internet connection without a login

**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. Open a web browser from a computer or mobile device that is connected to the
   access point/router network.

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

   If you are not connected to the access point/router network but to the same network
   as the access point/router, enter the IP address that is assigned to the access
   point/router. If you do not know the IP address, see <u>Find the IP address of the access
   point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign
   in with the local login credentials (see <u>Log in to the access point/router when it is
   not connected to the Internet</u> on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **BASIC > Internet**.
    The Internet Setup page displays.

6. Select the **No** radio button.
    This is the default setting.

7. 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 WAC124.

8. If your Internet connection requires a domain name, enter it in the **Domain Name** field.
    For the other sections on this page, the default settings usually work, but you can change them.

9. 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/router.
    *   **Use Static IP Address**. Enter the static IP address, IP subnet mask, and gateway IP address that your ISP assigned to the access point/router. The gateway is the ISP router to which the access point/router connects.

10. 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/router.
    *   **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.

11. Select a Router MAC Address radio button:

    *   **Use Default Address**. Use the default access point/router MAC address that displays on the Dashboard page and the access point/router label.
    *   **Use Computer MAC Address**. The access point/router 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.

12. Click the **Apply** button.

    Your settings are saved.

13. 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:

    - Router mode: You cannot access the Internet on page 248

    - Troubleshoot Internet browsing on page 251

Router mode: Specify a PPPoE Internet connection that uses a login

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

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

    The BASIC Home page displays.

5. Select **BASIC > Internet**.

    The Internet Setup page displays.

6. Select the **Yes** radio button.

The settings on the page change.

7. From the **Internet Service Provider** menu, select **PPPoE** as the encapsulation method.

8. In the **Login** field, enter the login name that your ISP gave you.

   This login name is often an email address.

9. In the **Password** field, enter the password that you use to log in to your Internet service.

10. If your ISP requires a service name, type it in the **Service Name** field.

11. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.

12. 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/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.

13. 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/router.
    - **Use Static IP Address**. Enter the static IP address, IP subnet mask, and gateway IP address that your ISP assigned to the access point/router. The gateway is the ISP router to which the access point/router connects.

14. 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/router.
    - **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.

15. Select a Router MAC Address radio button:

    - **Use Default Address**. Use the default access point/router MAC address that displays on the Dashboard page and the access point/router label.
    - **Use Computer MAC Address**. The access point/router 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.

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:

    • Router mode: You cannot access the Internet on page 248

    • Troubleshoot Internet browsing on page 251

Router mode: Specify a PPTP or L2TP Internet connection that uses a login

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

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **BASIC > Internet**.

   The Internet Setup page displays.

6. Select the **Yes** radio button.

   The settings on the page change.

7. From the **Internet Service Provider** menu, select **PPTP** or **L2TP** as the encapsulation method.

8. In the **Login** field, enter the login name that your ISP gave you.

    This login name is often an email address.

9. In the **Password** field, enter the password that you use to log in to your Internet service.

10. If your ISP requires a service name, type it in the **Service Name** field.

11. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.

12. 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.

13. 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.

14. 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/router.
    • **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.

15. Select a Router MAC Address radio button:

    • **Use Default Address**. Use the default access point/router MAC address that displays on the Dashboard page and the access point/router label.
    • **Use Computer MAC Address**. The access point/router 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.

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:

    - Router mode: You cannot access the Internet on page 248

    - Troubleshoot Internet browsing on page 251

Router mode: Specify an IPv6 Internet connection

If the access point/router is in router mode, you can set up an IPv6 Internet connection if the router does not detect it automatically.

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

To set up an IPv6 Internet connection:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.
    The Sign-In page displays. You are prompted to sign in with your NETGEAR account. If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > IPv6**.
    The IPv6 page displays.

6. From the **Internet Connection Type** menu, select the IPv6 connection type:

    - If your Internet service provider (ISP) did not provide details, select **6to4 Tunnel**.

- If you are not sure, select **Auto Detect** so that the access point/router detects the IPv6 type that is in use.

- If your Internet connection does not use PPPoE or DHCP, or is not fixed, but is IPv6, select **Auto Config**.

Your ISP can provide this information. For more information about IPv6 Internet connection, see the following sections:

- <u>Router mode: Use Auto Detect for an IPv6 Internet connection</u> on page 47
- <u>Router mode: Use Auto Detect for an IPv6 Internet connection</u> on page 47
- <u>Router mode: Set up an IPv6 6to4 tunnel Internet connection</u> on page 51
- <u>Router mode: Set up an IPv6 6rd Internet connection</u> on page 52
- <u>Router mode: Set up an IPv6 passthrough Internet connection</u> on page 54
- <u>Router mode: Set up an IPv6 fixed Internet connection</u> on page 55
- <u>Router mode: Set up an IPv6 DHCP Internet connection</u> on page 57
- <u>Router mode: Set up an IPv6 PPPoE Internet connection</u> on page 58

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

Router mode: Requirements for entering IPv6 addresses

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

Router mode: Use Auto Detect for an IPv6 Internet connection

To set up an IPv6 Internet connection through autodetection:

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

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

If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > IPv6**.
    The IPv6 page displays.

6. From the **Internet Connection Type** menu, select **Auto Detect**.
    The page adjusts. The access point/router 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/router'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/router'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.

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/router 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/router's LAN interface.

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

9. Click the **Apply** button.

   Your settings are saved.

Router mode: Use Auto Config for an IPv6 Internet connection

To set up an IPv6 Internet connection through autoconfiguration:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

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

   The IPv6 page displays.

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

   The page adjusts. The access point/router 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/router'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/router'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.

7. (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.

8. (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.

9. 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.

10. 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/router assigns IPv6 addresses to the
    devices on your home network (the LAN).

11. (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/router's
    LAN interface.

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

12. Click the **Apply** button.

    Your settings are saved.

Router mode: Set up an IPv6 6to4 tunnel Internet connection

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.

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

   The page adjusts. The access point/router 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/router'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.

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

   - **Auto**. Your access point/router 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.

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/router 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/router's LAN interface.

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

11. Click the **Apply** button.

    Your settings are saved.

Router mode: Set up an IPv6 6rd Internet connection

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/router 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/router receives option 212 from the DHCPv4 option, autodetect selects the IPv6 as 6rd tunnel setting (see Router mode: Use Auto Detect for an IPv6 Internet connection on page 47).

The access point/router uses the 6rd option information to establish the 6rd connection.

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

To set up an IPv6 6rd Internet connection:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.

6. From the **Internet Connection Type** menu, select **6rd Tunnel**.
   The page adjusts. The access point/router automatically detects the information in the following sections:

   - **6rd (IPv6 Rapid Development) Configuration**. The access point/router 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/router, the page adjusts to display the correct settings in this section.

     Note: If the access point/router 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/router'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.

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/router 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/router's LAN interface.

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

10. Click the **Apply** button.

    Your settings are saved.

Router mode: Set up an IPv6 passthrough Internet connection

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/router does not process any IPv6 header packets.

To set up a pass-through IPv6 Internet connection:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.

6. From the **Internet Connection Type** menu, select **Pass Through**.
   The page adjusts, but no additional fields display.

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

Router mode: Set up an IPv6 fixed Internet connection

To set up a fixed IPv6 Internet connection:

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

2. Enter **http://www.routerlogin.net** in the address field.
   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

    The IPv6 page displays.

6. From the **Internet Connection Type** menu, select **Fixed**.

    The page adjusts.

7. 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/router's WAN interface.

    •   **Default IPv6 Gateway**. The IPv6 address of the default IPv6 gateway for the access point/router's WAN interface.

    •   **Primary DNS Server**. The primary DNS server that resolves IPv6 domain name records for the access point/router.

    •   **Secondary DNS Server**. The secondary DNS server that resolves IPv6 domain name records for the access point/router.

    Note: If you do not specify the DNS servers, the access point/router uses the DNS servers that are configured for the IPv4 Internet connection on the WAN Setup page. (See <u>Router mode: Manually set up the access point/router Internet connection</u> on page 40.)

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/router assigns IPv6 addresses to the devices on your home network (the LAN).

9. In the LAN Setup section, in the **IPv6 Address/Prefix Length** fields, specify the static IPv6 address and prefix length of the access point/router's LAN interface.

10. Click the **Apply** button.

    Your settings are saved.

Router mode: Set up an IPv6 DHCP Internet connection

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

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.

6. From the **Internet Connection Type** menu, select **DHCP**.
   The page adjusts. The access point/router 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/router'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/router'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.

7. (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.

8. (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.

9. 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.

10. 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/router assigns IPv6 addresses to the devices on your home network (the LAN).

11. (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/router's LAN interface.

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

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

Router mode: Set up an IPv6 PPPoE Internet connection

To set up a PPPoE IPv6 Internet connection:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

    The BASIC Home page displays.

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

    The IPv6 page displays.

6. From the **Internet Connection Type** menu, select **PPPoE**.

    The page adjusts. The access point/router 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/router'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/router'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.

7. Specify the PPPoE settings for IPv6:

    • **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/router never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the access point/router 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/router 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/router's LAN interface.

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

11. Click the **Apply** button.

   Your settings are saved.

4

Manage the Basic WiFi and Radio Features

This chapter describes how you can manage the basic WiFi and radio settings of the access point/router. For information about the advanced WiFi and radio settings, see Manage the Advanced WiFi and Radio Features on page 209.

Tip: If you want to change the settings of the access point/router's WiFi network, 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
- Disable or enable a WiFi network
- Hide or broadcast the SSID for a WiFi network
- Enable or disable the WiFi radios
- Use WPS to add a device to the WiFi network

Set up or change an open or secure WiFi network

The access point/router provides three WiFi networks (Wireless 1, Wireless 2, and Wireless 3). By default, the Wireless 1 network is enabled (the other two WiFi networks are disabled), its default SSID is NETGEAR-1, and its default security is WPA2-PSK with the passphrase **sharedsecret**.

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.

For each WiFi network, the access point/router simultaneously supports the 2.4 GHz band for 802.11b/g/n devices and the 5 GHz band for 802.11a/n/ac devices. For the 2.4 GHz band, the default WiFi throughput mode is 300 Mbps. For the 5 GHz band, it is 1733 Mbps. You can change (lower) the WiFi throughput mode (see Change the WiFi throughput mode for a radio band on page 212).

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

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. From the **Region** menu, select the region in which the access point/router operates. For some countries, 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.

Note: It might not be legal to operate the access point/router 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.

7. Select the WiFi network (**Wireless 1**, **Wireless 2**, or **Wireless 3**).
8. View, enable, or change the basic WiFi settings and security settings for the selected WiFi network.

   The following table describes the fields for the WiFi network.

Setting	Description
VAP	Select the **Enable** radio button to enable the WiFi network, also referred to as a virtual access point (VAP) 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.
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.
Name (SSID)	The SSID (service set identifier) is the WiFi network name. If you do not change the SSID, the default SSID (NETGEAR-1, NETGEAR-2, or NETGEAR-3) displays. The default SSID is also printed on the access point/router label (see Access point/router label on page 14). **Note:** If you change the SSID, enter a 32-character (maximum), case-sensitive name in this field.

(Continued)

Setting	Description
Enable SSID Broadcast	By default, the access point/router 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 of the access point/router.
Security Options	If you change the WiFi security, select one of the following WiFi security options for the access point/router's WiFi network:

- **None**. An open WiFi network does not provide any security. Any WiFi device can join the network. We recommend that you do *not* use an open WiFi network but configure WiFi security.

- **WPA2-PSK [AES]**. For the Wireless 1 network, this option is the default setting and the default WiFi passphrase (sharedsecret) is printed on the access point/router label (see Access point/router label on page 14). For the Wireless 2 and Wireless 3 networks, if you do not change the passphrase, the default passphrase (sharedseceret) displays. This type of security enables WiFi devices that support WPA2 to join the access point/router's WiFi network. WPA2 provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select WPA-PSK [TKIP] + WPA2-PSK [AES] security.
  If you change the passphrase, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the access point/router's WiFi network, a user must enter this passphrase.

- **WPA-PSK [TKIP] + WPA2-PSK [AES]**. This type of security enables WiFi devices that support either WPA or WPA2 to join the access point/router's WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps.
  To use this type of security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the access point/router's WiFi network, a user must enter this passphrase.

- **WPA/WPA2 Enterprise**. This type of security requires that your WiFi network can access a RADIUS server. For information about configuring WPA/WPA2 Enterprise, see Configure WPA and WPA2 Enterprise WiFi security on page 65.

9. 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.

10. 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 WiFi-enabled computer or mobile 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/router provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
- If your WiFi-enabled computer or mobile 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 WiFi device display as an attached device? (See View devices currently on the access point/router network on page 153.) 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

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/router to provide WPA and WPA2 enterprise WiFi security, the WiFi network that the access point/router provides must be able to access a RADIUS server.

To configure WPA and WPA2 enterprise security:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

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

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

7. In the Security Options section, select the **WPA/WPA2 Enterprise** radio button.
   The WPA and WPA2 enterprise settings display.

8. In the WPA/WPA2 Enterprise section, enter the settings as described in the following table.

Field	Description
Encryption mode	From the **Encryption Mode** menu, select the enterprise mode: • **WPA [TKIP] +WPA2 [AES]**. This type of security enables WiFi devices that support either WPA or WPA2 to join the access point/router's WiFi network. This is the default mode. • **WPA2 [AES]**. WPA2 provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select WPA [TKIP] + WPA2 [AES] security.
Group Key Update Interval	Enter the interval in seconds after which the RADIUS group key is updated. The default interval is 3600 seconds.
RADIUS Server IP Address	Enter the IPv4 address of the RADIUS server to which the WiFi network can connect.
RADIUS Server Port	Enter the number of the port on the access point/router that is used to access the RADIUS server for authentication. The default port number is 1812.
Shared Key	Enter the shared key (RADIUS password) that is used between the access point/router and the RADIUS server during authentication of a WiFi client.

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

10. 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 WiFi-enabled computer or mobile 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/router provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.

- If your WiFi-enabled computer or mobile 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 WiFi device display as an attached device? (See View devices currently on the access point/router network on page 153.) If it does, it is connected to the network.
- Are you using the correct network name (SSID) and password?

Disable or enable a WiFi network

You can temporarily disable a WiFi network (that is, an SSID or VAP) and you can reenable 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 210. For information about turning off the radios entirely (and, therefore, all WiFi networks), see Enable or disable the WiFi radios on page 69.

To disable or enable a WiFi network:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

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

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

7. 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.

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

Hide or broadcast the SSID for a WiFi network

By default, a WiFi network (SSID or VAP) 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

2. Enter **http://www.routerlogin.net** in the address field.
   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

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

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

7. 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.

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

Enable or disable the WiFi radios

The access point/router provides 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/router. When both WiFi radios are off, you can still use an Ethernet cable for a LAN connection to the access point/router.

You can also turn the WiFi radios one and off based on a schedule. (See Add a WiFi schedule for a radio on page 210.)

To enable or disable one or both WiFi radios:

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

2. Enter **http://www.routerlogin.net** in the address field.
    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

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

6. Do one of the following in the 2.4 GHz b/g/n wireless radio settings section, 5 GHz a/n/ac wireless radio settings section, or both sections:

    • **Turn off the radio**. Clear the **Enable Wireless Router Radio** check box.
      The WiFi LED turns off.
    • **Turn on the radio**. Select the **Enable Wireless Router Radio** check box.
      The WiFi LED lights solid green.

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

Use WPS to add a device to the WiFi network

WPS (Wi-Fi Protected Setup) lets you connect a computer or mobile device to the access point/router'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 <u>Set up or change an open or secure WiFi network</u> on page 62).

Use WPS with the push button method

For you to use the push button method to connect a WiFi device to the access point/router'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 let a WiFi device join the access point/router's main WiFi network using WPS with the push button method:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > WPS Wizard**.
   The Add WPS Client page displays and shows a description of the WPS method.

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

7. Either click the button onscreen or press the **WPS** button on the rear panel of the access point/router.
   For two minutes, the access point/router attempts to find the WiFi device (that is, the client) that you want to join the access point/router's main WiFi network.

   During this time, the WiFi LED on the top panel of the access point/router blinks slowly.

8. Within two minutes, go to the WiFi device and press its **WPS** button to join the access point/router's main WiFi network without entering a password.
   After the access point/router establishes a WPS connection, the WiFi LED lights and the Add WPS Client page displays a confirmation message.

9. To verify that the WiFi device is connected to the access point/router'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/router's WiFi network, you must know the PIN of the WiFi device that you are trying to connect.

To let a WiFi device join the access point/router's WiFi network using WPS with the PIN method:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

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

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

6. Click the **Next** button.

   The Add WPS Client page adjusts.

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

7. Select the **PIN Number** radio button.

8. In the **Enter Clients' PIN** field, enter the PIN number of the WiFi device.

9. Click the **Next** button.

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

During this time, the WiFi LED on the top panel of the access point/router blinks.

10. 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/router establishes a WPS connection, the WiFi LED lights and the Add WPS Client page displays a confirmation message.

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

    The WiFi device displays on the page.

5

Manage the Firewall and Security

The access point/router 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:

Router mode: Manage the basic firewall settings

If the access point/router 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/router can respond to a ping from the 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 Router mode: Change the MTU size on page 128.

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

Router mode: Manage port scan protection and denial of service protection

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/router to respond to a ping to its WAN (Internet) port. This feature allows your access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Setup > WAN Setup**.

   The WAN Setup page displays.

6. To enable a port scan and disable DoS protection, select the **Disable Port Scan and DoS Protection** check box.

7. To enable the access point/router to respond to a ping on its WAN port, select the **Respond to Ping on Internet Port** check box.

8. Click the **Apply** button.

   Your settings are saved.

Router mode: Set up a default DMZ server

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/router 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/router 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 Router Mode: Manage Port Forwarding and Port Triggering on page 224). Instead of discarding this traffic, you can direct the access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

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

---

point/router. If you do not know the IP address, see <u>Find the IP address of the access</u> <u>point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is</u> <u>not connected to the Internet</u> on page 28).

3. Click the **Login** button.
The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
The BASIC Home page displays.

5. Select **ADVANCED > Setup > WAN Setup**.
The WAN Setup page displays.

6. Select the **Default DMZ Server** check box.

7. Enter the LAN IP address of the computer that must function as the DMZ server.

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

Router mode: Manage IGMP proxying

IGMP proxying allows a computer or mobile device on the access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access</u> <u>point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is</u> <u>not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Setup > WAN Setup**.

   The WAN Setup page displays.

6. Clear the **Disable IGMP Proxying** check box.

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

7. Click the **Apply** button.

   Your settings are saved.

Router mode: Manage NAT filtering

Network Address Translation (NAT) determines how the access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Setup > WAN Setup**.

   The WAN Setup page displays.

6. 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.

7. Click the **Apply** button.

   Your settings are saved.

Router mode: Manage the SIP application-level gateway

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/router provides the option to disable the SIP ALG.

To change the default SIP ALG setting:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Setup > WAN Setup**.

The WAN Setup page displays.

6. To disable the SIP ALG, select the **Disable SIP ALG** check box.
   The SIP ALG is enabled by default.

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

Router mode: Manage VPN pass-through

VPN pass-through allows a computer on the local area network (LAN) to receive VPN traffic from the Internet over an IPSec, PPTP, or L2TP connection. Under normal circumstances, leave VPN pass-through enabled, which is the default setting. If you disable VPN pass-through, VPN traffic is blocked.

To disable VPN pass-through:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.

6. In the VPN Passthrough section, select one or more **Disabled** radio buttons.
   By default, the **Enable** radio buttons are selected and VPN pass-through is enabled for IPSec, PPTP, and L2TP.

7. Click the **Apply** button.

Your settings are saved.

Allow or block device access to your network

You can use device access control to block or allow access to your network. You define access by selecting or specifying the MAC addresses of the WiFi and wired devices that either can access your entire network or are blocked from accessing your entire network.

Enable and manage network access control

When you enable access control, you must select whether new devices are allowed to access the access point/router 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.

To set up network access control:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Security > Access Control**.

   The Access Control page displays.

6. 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.

7. Click the **Apply** button.

    Your settings are saved.

8. Select an access rule for new devices:

    - **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 Manage network access control lists on page 82.

    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.

9. To manage access for currently connected computers and devices, do the following:

    a. If you blocked all new devices, you can allow the computer or device that you are currently using to continue to access the network. Select the check box next to your computer or device in the table, and click the **Allow** button.

    b. To change the allow or block settings for other computers and devices, select the check box next to the computer or device in the table, and click either the **Allow** button or the **Block** button.

10. Click the **Apply** button.

    Your settings are saved.

Manage 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 mobile devices that can either access your entire network or are blocked from accessing your entire network.

The access point/router 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/router on the Access Control page of the local browser interface (see Add or remove a device from

Add or remove a device from the allowed list

If you set up an access list that blocks all new devices from accessing your network, you must specify which devices are allowed to access your network.

To add or remove a device from the allowed list:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Security > Access Control**.
   The Access Control page displays.

6. 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.

7. 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. On the Add Allowed Device page, click the **Apply** button.
      The device is added to the allowed list on the Access Control page.

8. To remove a device from the allowed list, do the following:

    a. Select the check box for the device.

    b. Click the **Delete** button.
       The device is removed from the allowed list.

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

Add or remove a device from the blocked list

If you set up an access list that allows all new devices to access your network but you want to block some devices, you must specify the devices that you want to block.

To add or remove a device from the blocked list:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Security > Access Control**.
   The Access Control page displays.

6. 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.

7. 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. On the Add Blocked Device page, click the **Apply** button.
      The device is added to the blocked list on the Access Control page.

8. To remove a device from the blocked list, do the following:

   a. Select the check box for the device.

   b. Click the **Delete** button.
      The device is removed from the blocked list.

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

Router mode: Specify keywords and domains to block Internet sites

If the access point/router is in router mode, you can block keywords and domains (websites) to prevent certain types of HTTP traffic from accessing your network. 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/router is in access point mode.

Router mode: Set up keyword and domain blocking

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

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

point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Security > Block Sites**.
   The Block Sites page displays.

6. Specify a keyword blocking option:

   • **Per Schedule**. Use keyword blocking according to a schedule that you set.
     For more information, see <u>Router mode: Set up a schedule for blocking</u> on page 95.

   • **Always**. Use keyword blocking continuously.

7. 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, .edu or .gov) if you want to allow only sites with domain suffixes such as .edu or .gov.

   • Enter a period (**.**) to block all Internet browsing access.

8. 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).

9. To add more keywords or domains, repeat the previous two steps.
   The keyword list supports up to 32 entries.

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

Router mode: Specify a trusted device

You can exempt one trusted device from blocking and logging. The device that you exempt must be assigned a fixed (static) IP address.

To specify a trusted device:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Security > Block Sites**.
   The Block Sites page displays.

6. Scroll down and select the **Allow trusted IP address to visit blocked sites** check box.

7. In the **Trusted IP Address** field, enter the IP address of the trusted device.
   The first three octets of the IP address (by default, 192.168.0) are automatically populated and depend on the IP address that is assigned to the DHCP server of the access point/router. For more information, see <u>Router mode: Manage the DHCP server address pool</u> on page 114.

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

Router mode: Remove a keyword or domain from the blocked list

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Security > Block Sites**.
   The Block Sites page displays.

6. In the **Block sites containing these keywords or domain names** field, select the keyword or domain.

7. Click the **Delete Keyword** button.
   The keyword or domain is removed from the blocked list.

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

Router mode: Remove all keywords and domains from the blocked list

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

To remove all keywords and domains from the blocked list:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > Security > Block Sites**.
    The Block Sites page displays.

6. Click the **Clear List** button.
    All keywords and domains are removed from the blocked list.

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

Router mode: Block specific services and applications from the Internet

If the access point/router 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/router 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/router is in access point mode.

Router mode: Add a service blocking rule for a predefined service or application

The access point/router 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 service or application on the Internet.

To add a service blocking rule:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

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

6. In the Services Blocking section, specify how the access point/router applies outbound rules:

    • **Per Schedule**. Use service blocking according to a schedule that you set.

For more information, see <u>Router mode: Set up a schedule for blocking</u> on page 95.

- **Always**. Use service blocking continuously.

7. Click the **Add** button.

   The Add Services Blocking page displays.

8. 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 <u>Router mode: Add a service blocking rule for a custom service or application</u> on page 91).

9. 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.

10. Click the **Add** button.

    The new rule is added to the Service Table on the Block Services page.

Router mode: Add a service blocking rule for a custom service or application

If the 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

4. Click the **Login** button.

   The NETGEAR Account Login page displays.

5. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

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

   The Block Services page displays.

7. The first time that you add an outbound firewall rule, in the Services Blocking section, specify how the access point/router applies outbound rules:

   • **Per Schedule**. Use keyword blocking according to a schedule that you set.
     For more information, see <u>Router mode: Set up a schedule for blocking</u> on page 95.

   • **Always**. Use keyword blocking continuously.

8. Click the **Add** button.

   The Add Services Blocking page displays.

9. From the **Service Type** menu, select **User Defined**.

10. 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 for the service or application.

  - **Ending Port**. In the field, enter one of the following:

    - If the service or application uses a range of ports, enter the end port for the range.

    - If the service or application uses a single port, repeat the port number that you entered in the **Starting Port** field.

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

11. 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.

12. Click the **Add** button.
    The new rule is added to the Service Table on the Block Services page.

Router mode: Change a service blocking rule

You can change an existing service blocking rule.

To change a service blocking rule:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. In the Service Table, select the radio button for the rule.

7. Click the **Edit** button.
   The Edit Services Blocking page displays.

8. Change the settings.
   For more information about the settings, see <u>Router mode: Add a service blocking rule for a custom service or application</u> on page 91.

9. Click the **Apply** button.
   Your settings are saved. The modified rule displays in the Service Table on the Block Services page.

Router mode: Remove a service blocking rule

You can remove a service blocking rule that you no longer need.

To remove a service blocking rule:

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

2. Enter **http://www.routerlogin.net** in the address field.
   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

    The BASIC Home page displays.

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

    The Block Services page displays.

6. In the Service Table, select the radio button for the rule.

7. Click the **Delete** button.

    A warning pop-up window opens.

8. Click the **OK** button.

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

Router mode: Set up a schedule for blocking

If the access point/router 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 Router mode: Set up keyword and domain blocking on page 85), Internet service and application blocking (see Router mode: Block specific services and applications from the Internet 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

5. Select **ADVANCED > Security > Schedule**.

The Schedule page displays.

6. 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.

7. Click the **Apply** button.

Your settings are saved.

Set up security event email notifications

The access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Security > E-mail**.
   The E-mail page displays.

6. Select the **Turn E-mail Notification On** check box.

7. In the **Send to This 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.

8. 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.

9. 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.

10. To send email alerts over a secure connection, select the **Secure connection (use SSL)** check box.

11. 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.

12. 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.

13. To send logs based on a schedule, specify these settings:

    a. From **Send logs according to this schedule** menu, select the schedule type.

    b. From the **Day** menu, select the day.

    c. From the **Time** menu, select the time, and select the **am** or **pm** radio button.

14. 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/router memory. If the access point/router cannot email the log and the log buffer fills, the access point/router overwrites the log.

6

Optimize Performance

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

The chapter contains the following sections:

- <u>Optimize traffic with the default QoS rules</u>
- <u>Manage default and custom QoS rules</u>
- <u>Manage uplink bandwidth control</u>
- <u>Manage WiFi Multimedia (WMM) for a radio</u>
- <u>Improve network connections with Universal Plug and Play</u>

Optimize traffic with the default QoS rules

You can use Quality of Service (QoS) to assign different priorities to Internet traffic, applications, and services. The access point/router provides default QoS rules. You can add custom QoS rules and manage both default and custom QoS rules (see <u>Manage default and custom QoS rules</u> on page 101).

We recommend that you enable QoS if you use streaming Internet. However, when QoS assigns a high priority to streaming video, it also assigns lower priority to the rest of your Internet traffic. That means that other tasks such as downloading content from the Internet take longer.

To view the default QoS rules with their default priorities and turn on QoS:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.

   If you did not add any custom rules or change priorities, the QoS rules table displays the default QoS rules and their default priority queues, from the highest queue (Queue 1, the leftmost column) to the lowest priority Queue 4, (the rightmost column).

6. Select the **Turn Internet Access QoS On** check box.

7. Click the **Apply** button.
   Your settings are saved. The access point/router assigns traffic priorities according to the QoS rules and their priority queues.

Manage default and custom QoS rules

You can add custom QoS rules and change and remove both default and custom QoS rules. You can add QoS rules for services and applications but also for specific devices on your network.

Add a custom QoS rule for a service or application

If the service or application for which you want to assign a traffic priority is not part of the default QoS rules, you can add a custom QoS rule.

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

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.

6. Make sure that the **Turn Internet Access QoS On** check box is selected.

7. Make sure that the **QoS By Service** radio button is selected.

8. From the **Applications** menu, select **Add a new application**.
   The QoS - Priority Rules page displays.

9. Specify a new QoS rule for a service or application by completing the following information:

- **QoS Policy for**. Enter a name for the QoS rule.

- **Priority**. Select the priority (**Highest**, **High**, **Normal**, or **Low**) that must be assigned to the service or application.
  The priority selections correspond to the queue columns in the QoS rules table.

- **Connection Type**. Select the protocol (**TCP** or **UDP**) that is associated with the service or application.
  If you are unsure, select **TCP/UDP**.

- **Starting Port**. Enter the start port number for the service or application.

- **Ending Port**. Enter the end port number for the service or application.

10. On the QoS - Priority Rules page, click the **Apply** button.
    The new QoS rule is added to the QoS rules table.

11. On the QoS Setup page, click the **Apply** button.
    Your settings are saved.

Add a custom QoS rule for a device

You can assign a traffic priority to a device on your network.

To add a QoS rule for a device:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

5. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.

6. Make sure that the **Turn Internet Access QoS On** check box is selected.

7. Select the **By Device** radio button.
   The page adjusts and shows the Add Rules table.

8. Either select the radio button for a device in the Add Rules table to complete the fields automatically (by default, each device is assigned a normal priority, but you can change that priority) or specify the settings for the device by completing the following information under the Add Rules table:

   • **QoS Policy for**. Enter a name for the QoS rule.

   • **MAC Address**. Enter the MAC address of the device.

   • **Device**. Enter the name for the device.

   • **Priority**. Select the priority (**Highest**, **High**, **Normal**, or **Low**) that must be assigned to the device.

9. Click the **Add** button.
   A QoS rule is added for the device to the QoS rules table.

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

Change a QoS rule or change the priority for a rule

You can change an existing default or custom QoS rule. For default rules, you can change the priority only. For custom rules, you can change the priority and other settings.

To change a QoS rule:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Setup > QoS Setup**.

   The QoS Setup page displays.

6. Make sure that the **Turn Internet Access QoS On** check box is selected.

7. In the QoS rules table, click the service, application, or device to select it.

   The **Edit** button becomes available.

8. Click the **Edit** button.

   The QoS Priority Rules page displays.

9. Change the settings.

   For more information about the settings, see <u>Add a custom QoS rule for a service or application</u> on page 101 or <u>Add a custom QoS rule for a device</u> on page 102.

10. On the QoS - Priority Rules page, click the **Apply** button.

    Your settings are saved. If you changed the priority, the QoS rule now displays in a different column of the QoS rules table on the QoS Setup page.

Remove a QoS rule

You can remove an individual custom or default QoS rule.

To remove a QoS rule:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

5. Select **ADVANCED > Setup > QoS Setup**.

The QoS Setup page displays.

6. In the QoS rules table, click the service, application, or device to select it.

The **Delete** button becomes available.

7. Click the **Delete** button.

The QoS rule is removed.

Remove all QoS rules

You can permanently remove all custom and default QoS rules.

Warning: If you remove all QoS rules, both the custom and default QoS rules are permanently removed. The only way to get the default QoS rules back is by returning the access point/router to factory default settings.

To remove all QoS rules:

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

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

If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > Setup > QoS Setup**.
    The QoS Setup page displays.

    Warning: If you click the **Delete All** button, all default and custom QoS rules are permanently removed.

6. Click the **Delete All** button.
    All QoS rules are permanently removed.

Manage uplink bandwidth control

Uplink bandwidth control lets you check the maximum uplink bandwidth that your Internet connection can support and specify the maximum uplink bandwidth.

To specify the maximum uplink bandwidth:

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

2. Enter **http://www.routerlogin.net** in the address field.
    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > Setup > QoS Setup**.
    The QoS Setup page displays.

6. To find out what uplink bandwidth your Internet connection supports, click the **Speedtest** button.

    The speed test checks your uplink bandwidth and the supported uplink bandwidth displays in the **Uplink bandwidth Maximum** field. Depending on your Internet speed, this process might take up to one minute.

7. In the **Uplink bandwidth Maximum** field, leave the detected bandwidth or enter the maximum uplink bandwidth that you want to specify.

8. From the associated menu, leave the detected units or select **Kbps** or **Mbps**.

9. Click the **Apply** button.

    Your settings are saved.

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

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

point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.

6. Clear the **Enable WMM (Wi-Fi multimedia) settings** check box the radio for which you want to disable WWM, 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

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 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.

Note: The UPnP Portmap Table displays only if the access point/router is in router mode.

To manage Universal Plug and Play:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > UPnP**.
   The UPnP page displays.

6. 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/router. For example, a device cannot control port forwarding on the access point/router.

7. Enter the advertisement period in minutes.

   The advertisement period specifies how often the access point/router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 3 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.

8. 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.

9. Click the **Apply** button.

    If the access point/router is in router mode, the UPnP Portmap Table displays the IP address of each UPnP device that is accessing the access point/router 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.

10. If the access point/router is in router mode, to refresh the information in the UPnP Portmap table, click the **Refresh** button.

7

Manage the Network Settings

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

The chapter includes the following sections:

- Router mode: Manage the LAN IP address settings
- Router mode: Manage reserved LAN IP addresses
- Add and manage IPv4 static routes
- Router mode: Enable an IPTV bridge for a port group or VLAN tag group
- Router mode: Change the MTU size

Router mode: Manage the LAN IP address settings

If the access point/router is in router mode, the LAN subnet defines the LAN IP address settings for the access point/router, including the IP address at which you can access the access point/router over the local browser interface, 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/router is in access point mode.

Router mode: Change the access point/router network device name

If the access point/router is in router mode, its default network device name is the model number (WAC124).

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

To change the router network device name:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Setup > LAN Setup**.

   The LAN Setup page displays.

6. Enter a new name in the **Device Name** field.

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

Router mode: Change the LAN IP address and subnet settings

If the access point/router 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/router's LAN IP configuration is as follows:

- **LAN IP address**. 192.168.0.100 (if the access point/router 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 <u>Router mode: Manage the DHCP server address pool</u> on page 114).

To change the LAN IP address and subnet settings:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. In the **IP Address** fields, enter the new LAN IP address.
   The LAN IP address at which you can access the local browser interface of the access point/router also changes.

7. 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 interface of the access point/router also changes.

8. 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 interface.

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

Router mode: Manage the DHCP server address pool

If the access point/router is in router mode, it functions as a Dynamic Host Configuration Protocol (DHCP) server. The access point/router 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/router's LAN IP address. The DHCP address pool for the LAN subnet is 192.168.0.2 through 192.168.0.254.

The access point/router 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/router assigns:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. Make sure that the **Use Router as DHCP Server** check box is selected.
   This check box is selected by default.

7. 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.

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

Router mode: Disable the DHCP server

If the access point/router 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/router.

To disable the DHCP server:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. Clear the **Use Router as DHCP Server** check box.

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

Router mode: Manage the Router Information Protocol settings

If the access point/router is in router mode, Router Information Protocol (RIP) lets the access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

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

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

7. 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.

8. Click the **Apply** button.

Your settings are saved.

Router mode: Manage reserved LAN IP addresses

If the access point/router 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/router'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/router is in access point mode.

Router mode: Reserve a LAN IP Address

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. Below the Address Reservation table, click the **Add** button.
   The Add Address page displays.

7. 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 router's LAN subnet, such as 192.168.0.x.
   • **MAC Address**. Enter the MAC address of the computer or device.
   • **Device Name**. Enter the name of the computer or device.

8. 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/router's DHCP server. Reboot the computer or device, or access its IP configuration and force a DHCP release and renew.

Router mode: Change a reserved LAN IP address

You can change an existing reserved LAN IP address.

To change a reserved LAN IP address:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

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

6. In the Address Reservation table, select the radio button for the reserved address.

7. Click the **Edit** button.
    The Address Reservation page displays.

8. Change the settings.

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

Router mode: Remove a reserved LAN IP address entry

You can remove a reserved LAN IP address entry that you no longer need.

To remove a reserved LAN IP address entry:

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

2. Enter **http://www.routerlogin.net** in the address field.
    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

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

6. In the Address Reservation table, select the radio button for the reserved address.

7. Click the **Delete** button.
   The IP address entry is removed.

Add and manage IPv4 static routes

Static routes provide detailed routing information to your router. 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 192.168.0.158.

- Your company's network address is 203.0.113.0.

When you first configured your access point/router, 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 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 203.0.113.0 network, your access point/router 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 192.168.0.158. 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 192.168.0.158.

- A metric value of 1 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Static Routes**.
   The Static Routes page displays.

6. Click the **Add** button.
   The Static Route page adjusts.

7. In the **Route Name** field, enter a name for the route.
   The name is for identification purposes.

8. To make the route private, select the **Private** check box.
   A private static route is not reported in RIP.

9. 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.

10. 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/router 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**.

11. 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Static Routes**.
   The Static Routes page displays.

6. In the Static Routes table, select the radio button for the route.

7. Click the **Edit** button.

   The Static Route page adjusts.

8. Change the settings for the route.

   For more information about the settings, see Add an IPv4 static route on page 122.

9. 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Static Routes**.

   The Static Routes page displays.

6. In the Static Routes table, select the radio button for the route.

7. Click the **Delete** button.

   The route is removed from the table on the Static Routes page.

Router mode: Enable an IPTV bridge for a port group or VLAN tag group

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

Note: If your ISP provides directions on how to set up a bridge for IPTV and Internet service, follow those directions.

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

Router mode: Enable an IPTV bridge for a port group

If the access point/router is in router mode and an IPTV device is connected to a LAN port or WiFi radio, your ISP might require you to set up a bridge for a port group for the access point/router's WAN (Internet) interface.

A bridge with a port group allows packets that are sent between the IPTV device and the access point/router WAN port to circumvent the access point/router's NAT service, which otherwise could drop the packets.

To enable the IPTV bridge for a port group:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.
   The VLAN / Bridge Settings page displays.

6. Select the **Enable VLAN/Bridge group** check box.
   The page expands.

7. Select the **By bridge group** radio button.
   The page adjusts.

8. Select the check box for the LAN port (**Port 1**, **Port 2**, **Port 3**, or **Port 4**) or WiFi radio
   (**WiFi-2.4G** or **WiFi-5G**) to which the IPTV device is connected.
   You must select at least one LAN port or one WiFi radio. You can select more than
   one LAN port and WiFi radio.

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

Router mode: Enable an IPTV bridge for a VLAN tag group

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

If you are subscribed to an IPTV service, the access point/router might require VLAN
tags 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/router WAN port to circumvent the access point/router's NAT service, which
otherwise could drop the packets.

The access point/router includes a default VLAN tag group with the name Internet, with
VLAN ID 10, and with all LAN ports, WiFi radios, and the WAN port as members. If you
enable the IPTV bridge for a VLAN tag group, this default VLAN tag group is also
enabled.

You can add custom VLAN tag groups and assign a VLAN ID, priority value, and ports
to each VLAN tag group.

To enable the IPTV bridge for a VLAN tag group:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.
   The VLAN / Bridge Settings page displays.

6. Select the **Enable VLAN Tag** check box.
   The page expands.

7. Select the **By VLAN tag group** radio button.
   The page adjusts and the default VLAN tag group displays.

8. To add a custom VLAN tag group, do the following:
   a. Click the **Add** button.
      The VLAN/IPTV Setup page displays.

   b. Specify the settings in the following fields:

      • **Name**. Enter a name for the VLAN tag group.
        The name is for identification purposes.

      • **VLAN ID**. Enter a value from 1 to 4094.

      • **Priority**. Enter a value from 0 to 7.

   c. Select the check box for the LAN port or WiFi radio to which the device is connected.

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

9. Click the **Apply** button.

    Your settings are saved. If you added a VLAN tag group, the group is added to the table on the VLAN / Bridge Settings page.

Router mode: Change the MTU size

If the access point/router 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 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Setup > WAN Setup**.
   The firewall Basic Setup page displays.

6. In the **MTU Size** field, enter a value from 616 to 1500.
   The default size is 1500 bytes.

7. 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 2. 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.)

Table 2. Common MTU sizes (Continued)

MTU	Application
1468	Used in some DHCP environments.
1436	Used in PPTP environments or with VPN.

8

Maintain and Monitor the Access Point/Router

This chapter describes how you can maintain the access point/router 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/router and its network traffic.

The chapter includes the following sections:

- Update the firmware of the access point/router
- Manage the configuration file of the access point/router
- Recover the local login admin password
- Return the access point/router to its factory default settings
- Manage the time settings
- Manage the activity log
- View the status and statistics of the access point/router
- Router mode: Monitor and meter Internet traffic
- Router mode: Manage and use remote access
- Change the system mode to router mode or back to access point mode
- Disable LED blinking or turn off LEDs

For information about changing the admin password for local login to the access point/router password and setting up password recovery, see the following sections in another chapter:

- Change the local login admin password on page 32
- Set up password recovery for the local login admin user name on page 33

Update the firmware of the access point/router

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

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

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

You can let the access point/router check 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/router using an Ethernet connection to update the firmware.

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

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. Click the **Check** button.

    The access point/router finds new firmware information if any is available and displays a message asking if you want to download and install it.

7. Click the **Yes** button.

    The access point/router locates and downloads the firmware and begins the update.

    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/router. Wait until the access point/router 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/router restarts.

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

Check for new firmware manually and update the access point/router manually

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

To download new firmware manually and update the access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

6. Click the **Login** button.
   The NETGEAR Account Login page displays.

7. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

9. Locate and select the firmware file on your computer or mobile device:

   a. Click the **Choose File** button.

   b. Navigate to and select the firmware file
      The file ends in `.img`.

10. Click the **Upload** button.
    A warning pop-up window opens.

11. 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/router. Wait until the access point/router 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/router restarts.

12. Verify that the access point/router runs the new firmware version:

    a. Open a web browser from a computer or mobile device that is connected to the access point/router network.

    b. Enter **http://www.routerlogin.net** in the address field.
       The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    c. Click the **Login** button.
       The NETGEAR Account Login page displays.

    d. Enter your registered email address and password and click the **LOG IN** button.
       The BASIC Home page displays.

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

Manage the configuration file of the access point/router

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

Back up the access point/router configuration file

You can save a copy of the current configuration settings.

To back up the access point/router's configuration file:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Administration > Backup Settings**.
   The Backup Settings page displays.

6. Click the **Back Up** button.

7. Choose a location to store the file on your computer.
   The backup file ends in `.cfg`.

8. Follow the directions of your browser to save the file.

Restore the access point/router configuration 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Administration > Backup Settings**.
   The Backup Settings page displays.

6. Click the **Choose File** button and navigate to and select the saved configuration file.
   The backup file ends in `.cfg`.

7. Click the **Restore** button.
   A warning pop-up window opens

8. Click the **OK** button.
   The configuration is uploaded to the access point/router. When the restoration is complete, the access point/router 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/router. Wait until the access point/router finishes restarting and the Power LED turns solid green.

Recover the local login admin password

If you set up password recovery for the local login admin password (see Set up password recovery for the local login admin user name on page 33) and three local login failures occur, you can try to recover the login local password.

To recover your local login admin password when the access point/router is not connected to the Internet:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with the local login credentials.

3. Enter your local login credentials.

    If you enter incorrect credentials three times, you are prompted to enter the serial number of the access point/router. This option displays only if you set up password recovery for the local login admin password.
    The serial number is on the product label.

4. Enter the serial number of the access point/router.

5. Click the **Continue** button.

    A window opens requesting the answers to your security questions.

6. Enter the saved answers to your security questions.

7. Click the **Continue** button.

    A window opens and displays your recovered password.

8. Click the **Login again** button.

    A login window opens.

9. With your recovered password, log in to the access point/router.

Return the access point/router to its factory default settings

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

If the access point/router is in access point mode and you do not know the current IP address of the access point/router, 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/router, reset the access point/router to factory default settings.

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

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

After you reset the access point/router to factory default settings, the access point/router is in access point mode, the password for the local login user name admin is password, the login URL is www.routerlogin.net (if the access point/router does not get an IP address from a DHCP server, the IP address is 192.168.0.100), and the DHCP server is disabled. For a list of factory default settings, see Technical specifications on page 259.

Use the Reset button

Caution: This process erases all settings that you configured in the access point/router.

To reset the access point/router to factory default settings:

1. On the back of the access point/router, locate the **Reset** button.
2. Using a straightened paper clip, press and hold the recessed **Reset** button until the Power LED lights yellow, which takes about five seconds.
3. Release the **Reset** button.

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

Erase the settings to factory default settings

Caution: This process erases all settings that you configured in the access point/router.

To erase the settings:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Administration > Backup Settings**.
   The Backup Settings page displays.

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/router 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/router. Wait until the access point/router finishes restarting and the Power LED turns solid green.

Manage the time settings

By default, the access point/router receives its time settings from a NETGEAR Network Time Protocol (NTP) server. You can change to another NTP server or set the time zone manually.

Manually set the time zone and adjust the daylight saving time

The access point/router might detect the time zone automatically or you might need to adjust the time zone and daylight saving time settings. When the access point/router synchronizes its clock with a Network Time Protocol (NTP) server, the access point/router detects the correct date and time. If the access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

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

   The NTP Settings page displays.

6. From the **Time Zone** menu, select the time zone for the area in which the access point/router operates.

7. If the access point is in an area that observes daylight saving time, select the **Automatically adjust for daylight saving time** check box.

8. Click the **Apply** button.

   Your settings are saved.

   When the access point/router 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 NTP server

By default, the access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

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

   The NTP Settings page displays.
   By default, the **Use default NETGEAR NTP server** radio button is selected.

6. Select the **Set your preferred NTP server** radio button.

7. Enter the NTP server domain name or IP address in the **NTP server** field.

8. Click the **Apply** button.

   Your settings are saved.

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

Manage the activity log

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

Specify which activities the access point/router logs

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

To manage which activities are logged:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

5. Select **ADVANCED > Administration > Logs**.
    The Logs page displays.

6. 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 interface of the access point/router
    - 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
    - ReadySHARE access
    - VPN service

7. Clear the check boxes that correspond to the activities that you do not want to be logged.

8. 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

5. Select **ADVANCED > Administration > Logs**.

The Logs page displays.

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

The access point/router sends the logs to the email address that you specified for email notifications (see <u>Set up security event email notifications</u> on page 96).

7. To refresh the log entries onscreen, click the **Refresh** button.

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

View the status and statistics of the access point/router

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

Access point mode: View information about the access point/router, LAN port, and WiFi settings

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

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

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

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

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

point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED**.

   The ADVANCED Home page displays.

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

   • **Green flag**. The settings are fine and no problems exist. For a radio, the WiFi network is enabled and secured.

   • **Red X**. A problem exists or the connection is down. For a radio, the WiFi network is disabled or down.

   • **Orange exclamation mark**. The access point/router cannot get an Internet connection (for example, because a cable is disconnected), the WiFi network of a radio is enabled but open (that is, it is unprotected), or another situation occurred and requires your attention.

   The following tables describe the fields of the panes.

Field	Description
AP information pane	
Hardware Version	The access point/router hardware version, which is the model number WAC124.
Firmware Version	The access point/router firmware version. If you update the firmware, the version changes (see Update the firmware of the access point/router on page 132).
GUI Language Version	The access point/router language version for the local browser interface.

(Continued)

Field	Description
Serial Number	The serial number of the access point/router. This number does not change.
Operation mode	AP

Field	Description
LAN Port pane To change these settings, see <u>Use the Internet Setup Wizard</u> on page 38 or <u>Access point mode: Specify a fixed LAN IP address</u> on page 39	
MAC Address	The MAC address that applies to the access point/router WAN (Internet) port.
IP Address	The LAN IP address that the access point/router receives from an existing router in your network or the static (fixed) IP address that you manually configured.
Connection	The type of Internet connection that the access point/router uses, which can be DHCP Client (the default setting) or FixedIP.
IP Subnet Mask	The IP subnet mask that the access point/router uses.
Domain Name Server	The IP address of the Domain Name System (DNS) server that the access point/router uses.

Field	Description
Wireless Settings (2.4GHz) or **Wireless Settings (5GHz)** To change these settings, see <u>Manage the Basic WiFi and Radio Features</u> on page 61 and <u>Manage the Advanced WiFi and Radio Features</u> on page 209.	
Region	The country and region in which the access point/router is being used (see <u>Set up or change an open or secure WiFi network</u> on page 62).
Channel	The channel that the radio uses (see <u>Change the channel for a radio</u> on page 211).
Mode	The WiFi throughput mode that the radio uses (see <u>Change the WiFi throughput mode for a radio band</u> on page 212).
Wireless AP	Whether the virtual access point (VAP) of the default WiFi network (Wireless 1) is enabled or disabled (see <u>Disable or enable a WiFi network</u> on page 67).

(Continued)

Field	Description
Broadcast Name	Whether the default WiFi network (Wireless 1) broadcasts its SSID (see <u>Hide or broadcast the SSID for a WiFi network</u> on page 68).
Wi-Fi Protected Setup	Whether the access point/router keeps its existing WiFi settings when you use WPS to connect a device to the radio: • **Configured**. The access point/router keeps its existing WiFi settings. This is the default setting. • **Not configured**. The access point/router generates a random SSID and passphrase and changes the security mode to WPA/WPA2-PSK mixed mode. For more information, see <u>Manage the WPS settings</u> on page 216.

Router mode: View information about the access point/router, Internet port, and WiFi settings

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

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

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED**.

   The ADVANCED Home page displays.

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

   - **Green flag**. The settings are fine and no problems exist. For a radio, the WiFi network is enabled and secured.

   - **Red X**. A problem exists or the connection is down. For a radio, the WiFi network is disabled or down.

   - **Orange exclamation mark**. The access point/router cannot get an Internet connection (for example, because a cable is disconnected), the WiFi network of a radio is enabled but open (that is, it is unprotected), or another situation occurred and requires your attention.

   The following tables describe the fields of the panes.

Field	Description
Router Information pane	
Hardware Version	The access point/router hardware version, which is the model number WAC124.
Firmware Version	The access point/router firmware version. If you update the firmware, the version changes (see <u>Update the firmware of the access point/router</u> on page 132).
GUI Language Version	The access point/router language version for the local browser interface.
Serial Number	The serial number of the access point/router. This number does not change.
LAN Port	
MAC Address	The single MAC address that applies to all four access point/router LAN ports combined.

(Continued)

Field	Description
IP Address	The IP address that applies to all four access point/router LAN ports through which you can access the access point/router.
DHCP Server	If the access point/router is in router mode, whether the DHCP server of the access point/router is enabled (the default setting in router mode) or disabled (see Router mode: Disable the DHCP server on page 116).

Field	Description
Internet Port pane To change these settings, see, Use the Internet Setup Wizard on page 38 or Router mode: Manually set up the access point/router Internet connection on page 40.	
MAC Address	The MAC address that applies to the access point/router WAN (Internet) port.
IP Address	The WAN IP address that the access point/router receives from your Internet modem or ISP or the WAN IP address that you manually configured.
Connection	The type of Internet connection that the access point/router uses, which can be DHCP Client (the default setting), FixedIP, PPPoE, PPTP, or L2TP.
IP Subnet Mask	The IP subnet mask that the access point/router uses.
Domain Name Server	The IP address of the Domain Name System (DNS) server that the access point/router uses.

Field	Description
Wireless Settings (2.4GHz) or **Wireless Settings (5GHz)** To change these settings, see Manage the Basic WiFi and Radio Features on page 61 and Manage the Advanced WiFi and Radio Features on page 209.	
Region	The country and region in which the access point/router is being used (see Set up or change an open or secure WiFi network on page 62).
Channel	The channel that the radio uses (see Change the channel for a radio on page 211).
Mode	The WiFi throughput mode that the radio uses (see Change the WiFi throughput mode for a radio band on page 212).
Wireless AP	Whether the virtual access point (VAP) of the default WiFi network (Wireless 1) is enabled or disabled (see Disable or enable a WiFi network on page 67).

(Continued)

Field	Description
Broadcast Name	Whether the default WiFi network (Wireless 1) broadcasts its SSID (see <u>Hide or broadcast the SSID for a WiFi network</u> on page 68).
Wi-Fi Protected Setup	Whether the access point/router keeps its existing WiFi settings when you use WPS to connect a device to the radio: • **Configured**. The access point/router keeps its existing WiFi settings. This is the default setting. • **Not configured**. The access point/router generates a random SSID and passphrase and changes the security mode to WPA/WPA2-PSK mixed mode. For more information, see <u>Manage the WPS settings</u> on page 216.

Check the Internet connection status

To check the Internet connection status:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED**.

   The ADVANCED Home page displays.

6. In the LAN Port pane (in access point mode) or in the Internet Port pane (in router mode), click the **Connection Status** button.

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

    When the access point/router 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/router.
      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/router.

    - **Default Gateway**. The IP address for the default gateway that the access point/router 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/router.
      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.

7. When the access point/router 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.

8. To close the window, click the **Close Window** button.

Display Internet port statistics

To display Internet port statistics:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED**.
   The ADVANCED Home page displays.

6. In the LAN Port pane (in access point mode) or in the Internet Port pane (in router mode), click the **Show Statistics** button.
   The Show Statistics window opens and displays following information:

   - **System Up Time**. The time elapsed since the access point/router 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.

- **Poll Interval**. The interval at which the statistics are updated on this page.

7. To manage the polling, do one of the following:

- To change the polling frequency, 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.

View devices currently on the access point/router network

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

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

To display the attached wired, WiFi, and VPN devices:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **Attached Devices**.

   Wired devices are connected to the access point/router with Ethernet cables. WiFi devices are connected to the access point/router 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/router.

   The following tables describe the fields on the Attached Devices page.

Field	Description
Wired Devices	
Status	If access control is enabled (see Allow or block device access to your network on page 81), the access control status of the device in the network (Allowed or Blocked).
IP Address	The IP address that is assigned to the device when it joined the access point/router network. This address can change when a device is disconnected and rejoins the network.
MAC Address	The unique MAC address, which does not change.
Device Name	The device name, if detected.
Connection Type	For LAN devices, the connection type is always Wired.

Field	Description
2.4 GHz Wireless Devices and **5 GHz Wireless Devices**	
Status	If access control is enabled (see Allow or block device access to your network on page 81), the access control status of the device in the network (Allowed or Blocked).
SSID	The service set identifier (SSID) or WiFi network name that the WiFi device is using.
IP Address	The IP address that is assigned to the device when it joined the access point/router network. This address can change when a device is disconnected and rejoins the network.
MAC Address	The unique MAC address, which does not change.
Device Name	The device name, if detected.

The following information displays only if the access point/router is in router mode.

Field	Description
VPN Client Devices	
Device Name	The device name, if detected.

(Continued)

Field	Description
Local IP Address	The IP address that is assigned to the device when it joined the access point/router network. This address can change when a device is disconnected and rejoins the network.
Remote IP Address	The IP address of the device at the other side of the VPN tunnel.
Connection Time	The time that elapsed since the device connected to the access point/router.

6. To refresh the information onscreen, click the **Refresh** button.

   The information onscreen is updated.

Router mode: Monitor and meter Internet traffic

If the access point/router is in router mode, you can enable traffic metering to monitor the volume of Internet traffic that passes through the access point/router's 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/router is in access point mode.

Router mode: Start the traffic meter without traffic restrictions

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

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

point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Traffic Meter**.
    The Traffic Meter page displays.

6. Select the **Enable Traffic Meter** check box.
    By default, no traffic limit is specified and the traffic volume or connection time is not controlled.

7. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.

8. To start the traffic counter immediately, click the **Restart Counter Now** button.

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

    The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see <u>Router mode: View the Internet traffic volume and statistics</u> on page 159.

Router mode: Restrict Internet traffic by volume

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

2. Enter **http://www.routerlogin.net** in the address field.
    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access

point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Traffic Meter**.
   The Traffic Meter page displays.

6. Select the **Enable Traffic Meter** check box.

7. Select the **Traffic volume control by** radio button.

8. 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.

9. In the **Monthly Limit** field, enter how many MBytes (MB) per month are allowed.

10. 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.

11. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.

12. In the Traffic Control section, enter a value in minutes to specify when the access point/router issues a warning message before the monthly limit in hours is reached.
    This setting is optional. The access point/router issues a warning when the balance falls below the number of minutes that you enter. By default, the value is 0 and no warning message is issued.

13. Select one or more of the following actions to occur when the limit is reached:

   • **Turn the Internet LED to flashing green**. This setting is optional. When the traffic limit is reached, the Internet LED blinks green.
   • **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.

14. Click the **Apply** button.

Your settings are saved.

The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see <u>Router mode: View the Internet traffic volume and statistics</u> on page 159.

Router mode: Restrict Internet traffic by connection time

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Traffic Meter**.
The Traffic Meter page displays.

6. Select the **Enable Traffic Meter** check box.

7. Select the **Connection time control** radio button.

The access point/router must be connected to the Internet for you to be able to select the **Connection time control** radio button.

8. In the **Monthly Limit** field, enter how many hours per month are allowed.
The access point/router must be connected to the Internet for you to be able to enter information in the **Monthly Limit** field.

9. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.

10. In the Traffic Control section, enter a value in minutes to specify when the access point/router issues a warning message before the monthly limit in hours is reached.

    This setting is optional. The access point/router 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.

11. Select one or more of the following actions to occur when the limit is reached:

    - **Turn the Internet LED to flashing green**. This setting is optional. When the traffic limit is reached, the Internet LED blinks green.
    - **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.

12. Click the **Apply** button.

    Your settings are saved.

    The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see Router mode: View the Internet traffic volume and statistics on page 159.

Router mode: View the Internet traffic volume and statistics

If you enabled the traffic meter (see Router mode: Start the traffic meter without traffic restrictions on page 155), you can view the Internet traffic volume and statistics.

To view the Internet traffic volume and statistics shown by the traffic meter:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Traffic Meter**.

   The Traffic Meter page displays.

6. 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.

7. To refresh the information onscreen, click the **Refresh** button.

   The information is updated.

8. 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 opens.

Router mode: Unblock the traffic meter after the traffic limit is reached

If 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Traffic Meter**.

   The Traffic Meter page displays.

6. In the Traffic Control section, clear the **Disconnect and disable the Internet connection** check box.

7. Click the **Apply** button.

   Your settings are saved.

Router mode: Manage and use remote access

If the access point/router is in router mode, you can access the access point/router over the Internet to view or change its settings. You must know the access point/router's WAN IP address to use this feature.

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

Router mode: Set up remote management for the access point/router

If the access point/router is in router mode, you can set up the remote management feature to access the access point/router's local browser interface securely over the Internet so that you can view or change its settings. You must know the access point/router's WAN IP address and access port to use this feature or use Dynamic DNS (see Router mode: Set up and manage Dynamic DNS on page 192).

To set up remote management:

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

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

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

point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Remote Management**.
   The Remote Management page displays.

6. Select the **Turn Remote Management On** check box.

7. In the Allow Remote Access By section, specify the external IP addresses to be allowed to access the router's remote management.

   Note: For enhanced security, restrict access to as few external IP addresses as practical.

   Select one of the following radio buttons and configure the options accordingly:

   • **Only This Computer**. To allow access from a single IP address on the Internet, select the **Only This Computer** radio button. Enter the IP address to be allowed access.
   • **IP Address Range**. To allow access from a range of IP addresses on the Internet, select the **IP Address Range** radio button. Enter a beginning and ending IP address to define the allowed range.
   • **Everyone**. To allow access from any IP address on the Internet, select the **Everyone** radio button. This radio button is selected by default.

8. Specify the port number for accessing the access point/router's local browser interface.
   The default port number is 8443, which is a common alternate for HTTPS. For greater security, you can enter a custom port number. Choose a number from 1024 to 65535, but do not use the number of any common service port.

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

The Remote Management Address field shows the IP address and port number at which you can access the access point/router remotely.

Router mode: Use remote access

To use remote access:

1. Open a web browser from a computer or mobile device that is *not* connected to the access point/router network.

2. Enter the access point/router's WAN IP address in the address field followed by a colon (:) and the custom port number.

   For example, if the external address of the access point/router is 203.0.113.123 and you use port number 8443 to access the access point/router, enter **http://203.0.113.123:8443** in the address field of the browser.

Change the system mode to router mode or back to access point mode

By default, the access point/router functions in access point mode, that is, the system mode is access point mode. Only *after* you complete the initial log-in process in access point mode, can you change the system mode to router mode and connect the access point/router to an Internet modem.

For information about the features that are enabled in router mode and disabled in access point mode, see <u>About router mode</u> on page 22.

The access point/router can function in one of the following system modes:

- **Access point mode**. By default, the access point/router functions in access point mode with its router functionality disabled. If the access point/router is in access point mode, you must connect the WAN (Internet) port of the access point/router to a LAN port on an existing network router in your network (see <u>Connect the access point/router to your existing router and log in for the first time</u> on page 17).

- **Router mode**. The access point/router functions in router mode with its router functionality enabled. If the access point/router is in router mode, you must connect the WAN (Internet) port of the access point/router to a LAN port on your Internet modem.

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

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Wireless Access Point**.
    The Wireless Access Point page displays.

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

    *   Select the **Enable Access Point Mode** radio button to let the access point/router function in access point mode.

    *   Clear the **Enable Access Point Mode** radio button to let the access point/router function in router mode.

    Note: When you change the system mode from router mode to access point mode, the features that are specific to router mode (see About router mode on page 22) are reset to factory default settings.

7. Click the **Apply** button.
    Your settings are saved. The access point/router restarts in the new system mode.

Disable LED blinking or turn off LEDs

The LEDs on the top panel of the access point/router indicate activities and behavior. You can disable LED blinking for network communications, or turn off all LEDs except the Power LED.

To disable LED blinking or turn off the LEDs:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. 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 <u>Top panel with LEDs</u> on page 12.

6. To disable blinking, select the **Disable blinking on Internet LED, Wireless LED and USB LED when data traffic is detected** radio button.

7. To turn off all LEDs except the Power LED, select the **Turn off all LEDs except Power LED** radio button.

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

9

Share a USB Storage Device Attached to the Access Point/Router

This chapter describes how to access and manage storage devices attached to your access point/router. ReadySHARE lets you access and share USB storage devices connected to the access point/router. (If your storage device uses special drivers, it is not compatible.)

Note: The USB port on the access point/router can be used only to connect a USB storage device such as a flash drive, hard drive, or printer. Do not connect a computer, USB modem, CD drive, or DVD drive to the access point/router USB port.

The chapter contains the following sections:

- USB device requirements
- Connect a USB storage device to the access point/router
- Access a USB storage device that is connected to the access point/router
- Map a USB storage device to a Windows network drive
- Back up a Windows-based computer with ReadySHARE Vault
- Back up a Mac with Time Machine
- Manage access to a USB storage device
- Enable FTP access within the access point/router network
- View and manage network folders on a USB storage device
- Router mode: Approve a USB storage device
- Safely remove a USB storage device

For more information about ReadySHARE features, visit netgear.com/readyshare.

USB device requirements

The access point/router works with most USB-compliant external flash and hard drives. For the most up-to-date list of USB devices that the access point/router supports, visit kb.netgear.com/app/answers/detail/a_id/18985/~/readyshare-usb-drives-compatibility-list.

Some USB external hard drives and flash drives require you to load the drivers onto the computer before the computer can access the USB storage device. Such USB storage devices do not work with the access point/router.

The access point/router supports the following file system types for full read/write access:

- FAT16
- FAT32
- NTFS
- NTFS with compression format enabled
- Ext2
- Ext3
- Ext4
- HFS
- HFS+

Connect a USB storage device to the access point/router

ReadySHARE lets you access and share a USB storage device that is connected to the USB port on the access point/router. (If your USB storage device uses special drivers, it is not compatible.)

To connect a USB storage device:

1. Insert your USB storage device into the USB port on the access point/router.

2. If your USB storage device uses a power supply, connect it.

   You must use the power supply when you connect the USB storage device to the access point/router.

   When you connect the USB storage device to the USB port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers and mobile on the access point/router network.

Access a USB storage device that is connected to the access point/router

From a computer or mobile device on the access point/router network, you can access a USB storage device that is connected to the access point/router.

Access a USB storage device from a Windows-based computer

To access a USB storage device that is connected to the access point/router from a Windows-based computer:

1. Connect a USB storage device to a USB port on your access point/router.

2. If your USB storage device uses a power supply, connect it.

   You must use the power supply when you connect the USB storage device to the access point/router.

   When you connect the USB storage device to the access point/router's port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers and mobile devices on the access point/router network.

3. Select **Start > Run**.

4. Enter **\\readyshare** in the dialog box.

5. Click the **OK** button.

   A window automatically opens and displays the files and folders on the USB storage device.

Access a USB storage device from a Mac

To access a USB storage device that is connected to the access point/router from a Mac:

1. Connect a USB storage device to a USB port on your access point/router.

2. If your USB storage device uses a power supply, connect it.

   You must use the power supply when you connect the USB storage device to the access point/router.

Attached to the Access
Point/Router

168

User Manual

When you connect the USB storage device to the access point/router's port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers and mobile devices on the access point/router network.

3. On a Mac that is connected to the network, select **Go > Connect to Server**.

   The Connect to Server window opens.

4. In the **Server Address** field, enter **smb://readyshare**.

5. When prompted, select the **Guest** radio button.

   If you set up access control on the access point/router and you allowed your Mac to access the access point/router network, select the **Registered User** radio button and enter **admin**. The password for admin is the same password that you use for local login to the access point/router. If you did not yet change the default password for local login, enter **admin** as the user name and **password** as the password.

6. Click the **Connect** button.

   A window automatically opens and displays the files and folders on the USB storage device.

Map a USB storage device to a Windows network drive

To map the USB storage device that is connected to the access point/router to a Windows network drive:

1. Connect a USB storage device to a USB port on your access point/router.

2. If your USB storage device uses a power supply, connect it.

   You must use the power supply when you connect the USB storage device to the access point/router.

   When you connect the USB storage device to the access point/router's port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers and mobile devices on the access point/router network.

3. Select **Start > Run**.

4. Enter **\\readyshare** in the dialog box.

5. Click the **OK** button.

   A window automatically opens and displays the USB storage device.

6. Right-click the USB device and select **Map network drive**.

   The Map Network Drive window opens.

7. Select the drive letter to map to the new network folder.

8. Click the **Finish** button.

   The USB storage device is mapped to the drive letter that you specified.

9. To connect to the USB storage device as a different user, select the **Connect using different credentials** check box, click the **Finish** button, and do the following:

   a. Type the user name and password.

      Use the same credentials that you use for local login to the access point/router. If you did not yet change the default password for local login, enter **admin** as the user name and **password** as the password.

   b. Click the **OK** button.

Back up a Windows-based computer with ReadySHARE Vault

The access point/router comes with free backup software for Windows-based computers. Connect a USB hard disk drive (HDD) to the access point/router for centralized, continuous, and automatic backup.

The following operating systems support ReadySHARE Vault:

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

To back up a Windows-based computer:

1. Connect a USB HDD storage device to the USB port on the access point/router.

2. If your USB HDD uses a power supply, connect it.

   You must use the power supply when you connect the USB HDD to the access point/router.

   When you connect the USB HDD to the access point/router's port, it might take up to two minutes before it is ready for sharing. By default, the USB HDD is available to all computers and mobile devices on the access point/router network.

3. Download ReadySHARE Vault from <u>netgear.com/readyshare</u> and install it on the Windows-based computer.

4. Launch ReadySHARE Vault.

5. Use the dashboard or the **Backup** tab to set up and run your backup.

Back up a Mac with Time Machine

You can use Time Machine to back up a Mac onto a USB hard disk drive (HDD) that is connected to the access point/router's USB port. You can access the connected USB HDD from your Mac with a wired or WiFi connection to the access point/router network.

Set up a USB hard disk drive on a Mac

We recommend that you use a new USB hard disk drive (HDD) or format your existing USB HDD to perform the Time Machine backup for the first time. Use a blank partition to prevent any problems during backup using Time Machine. The access point/router supports GUID or MBR partitions.

To format your USB HDD and specify partitions:

1. Connect a USB HDD storage device to the USB port on the access point/router.

2. If your USB HDD uses a power supply, connect it.

   You must use the power supply when you connect the USB HDD to the access point/router.

   When you connect the USB HDD to the access point/router's port, it might take up to two minutes before it is ready for sharing. By default, the USB HDD is available to all computers and mobile devices on the access point/router network.

3. On your Mac, go to **Spotlight** (or the magnifying glass) at the top right of the page and search for Disk Utility.

4. Open the Disk Utility, select your USB HDD, click the **Erase** tab, and click the **Erase** button.

5. Click the **Partition** tab.

6. In the **Partition Layout** menu, set the number of partitions that you want to use.

7. Click the **Options** button.

   The Partition schemes display.

8. Select the **GUID Partition Table** or **Master Boot Record** radio button.

9. In the **Format** menu, select **Mac OS Extended (Journaled)**.

10. Click the **OK** button.

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

Prepare to back up a large amount of data

Before you back up a large amount of data with Time Machine, we recommend that you follow this procedure.

To prepare to back up a large amount of data:

1. Upgrade the operating system of the Mac.

2. Verify and, if needed, repair the backup disk and the local disk.

3. Verify and, if needed, repair the permissions on the local disk.

4. Set Energy Saver:

   a. From the **Apple** menu, select **System Preferences**.
      The System Preferences page displays.

   b. Select **Energy Saver**.
      The Energy Saver page displays.

   c. Click the **Power Adapter** tab.

   d. Select the **Wake for Wi-Fi network access** check box.

   e. Click the **back arrow** to save the changes and exit the page.

5. Modify your security settings:

   a. On the **System Preferences** page, select **Security & Privacy**.
      The Security & Privacy page displays.

   b. Click the **Advanced** button at the bottom of the page.
      If the **Advanced** button is masked out, click the lock icon so that you can change the settings.

   c. Clear the **Log out after minutes of inactivity** check box.

   d. Click the **OK** button.
      Your settings are saved.

Use Time Machine to back up onto a USB hard disk drive

You can use Time Machine to back up your Mac onto a USB hard disk drive (HDD) that is connected to USB port of the access point/router.

To back up your Mac onto a USB HDD:

1. Prepare your USB HDD with a compatible format and partitions.

   For more information, see <u>Set up a USB hard disk drive on a Mac</u> on page 171.

2. If you plan to back up a large amount of data, see <u>Prepare to back up a large amount of data</u> on page 172.

3. Connect a USB HDD storage device to the USB port on the access point/router.

4. If your USB HDD uses a power supply, connect it.

   You must use the power supply when you connect the USB HDD to the access point/router.

   When you connect the USB HDD to the access point/router's port, it might take up to two minutes before it is ready for sharing. By default, the USB HDD is available to all computers and mobile devices on the access point/router network.

5. On a Mac computer that is connected to the access point/router network, launch Finder and select **Go > Connect to Server**.

   The Connect to Server window opens.

6. Type **smb://routerlogin.net** and click the **Connect** button.

7. When prompted, select the **Registered User** radio button.

8. Enter the same credentials that you use for local login to the access point/router.

   If you did not yet change the default password for local login, enter **admin** as the user name and **password** as the password.

9. Click the **Connect** button.

   The USB HDD that is connected to the access point/router displays.

10. From the **Apple** menu, select **System Preferences**.

    The System Preferences window displays.

11. Select **Time Machine**.

    The Time Machine window displays.

12. Click the **Select Backup Disk** button and select your USB HDD from the list.

13. Click the **Use Disk** button.

    Note: If you do not see the USB partition that you want in the Time Machine disk list, go to Mac Finder and click that USB partition. It displays in the Time Machine list.

14. When prompted, select the **Registered User** radio button.

15. Enter the same credentials that you use for local login to the access point/router.

    If you did not yet change the default password for local login, enter **admin** as the user name and **password** as the password.

16. Click the **Connect** button.

When the setup is complete, the Mac automatically schedules a full backup. You can back up immediately.

Manage access to a USB storage device

You can specify the device name, workgroups, and network folders for a USB storage device that is connected to the USB port on the access point/router.

To specify access to the USB storage device:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > USB Storage > ReadySHARE**.
   The USB Storage (Advanced Settings) page displays.

6. To specify a name that is used to access the USB storage device that is connected to the access point/router, in the **Network/Device Name** field, enter a name.
   By default, the name is readyshare.

7. To specify a name for the workgroup that the USB storage device is a member of, in the **Workgroup** field, enter a name.

   By default, the name is Workgroup. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows. If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here.

8. Enable or disable access methods by selecting or clearing the corresponding check boxes and specifying access to the USB storage device as described in the following table.

Access Method	Description
Network Neighborhood/MacShare	Enabled by default. You can type **smb:\\readyshare** to access the USB storage device within the access point/router network. If you change the name in the **Network/Device Name** field from readyshare to another name, the link changes accordingly. You can enable password protection by selecting the **Admin Password Protection** check box.
HTTP	Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB storage device within the access point/router network and download or upload files. In this URL, readyshare is the name that is specified in the **Network/Device Name** field. If you change the name in the **Network/Device Name** field from readyshare to another name, the link changes accordingly. You can also click the link that is shown in the Link column. The fixed port is number is 80. You can enable password protection by selecting the **Admin Password Protection** check box.
HTTPS (via internet)	Disabled by default. If you enable this feature, remote users can type **https://**<public IP address>**/shares** to access the USB storage device over the Internet. <public IP address> is the external or public IP address that is assigned to the access point/router (for example, 1.1.10.102). This feature supports file uploading only. The default port is number 443, which you can change. Password protection is enabled by default.

(Continued)

Access Method	Description
FTP	Disabled by default. You can type **ftp://readyshare.routerlogin.net/shares** to access the USB storage device within the access point/router network and download or upload files. In this URL, readyshare is the name that is specified in the **Network/Device Name** field. If you change the name in the **Network/Device Name** field from readyshare to another name, the link changes accordingly. You can also click the link that is shown in the Link column. The fixed port is number is 21. You can enable password protection by selecting the **Admin Password Protection** check box.
FTP (via internet)	Disabled by default. If you enable this feature, remote users can type **ftp://**<public IP address>**/shares** to access the USB storage device over the Internet and download or upload files. <public IP address> is the external or public IP address that is assigned to the access point/router (for example, 1.1.10.102). The default port is number 21, which you can change. Password protection is enabled by default. If you set up Dynamic DNS, you can also type a URL domain name. For example, if your domain name is MyName and you use the NETGEAR DDNS server, you can type **ftp://MyName.mynetgear.com** to access the USB storage device over the Internet and download or upload files.

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

Enable FTP access within the access point/router network

File Transfer Protocol (FTP) lets you download (receive) and upload (send) large files faster.

Note: For information about using FTP to access a USB storage device through the Internet, see <u>Router mode: Use FTP to access a storage device over the Internet</u> on page 197.

To enable FTP access within the access point/router network:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > USB Storage > ReadySHARE**.

   The USB Storage (Advanced Settings) page displays.

   FTP is disabled by default.

6. Select the **FTP** check box.

   You can type **ftp://readyshare.routerlogin.net/shares** to access the USB storage device within the access point/router network and download or upload files. In this URL, readyshare is the name that is specified in the **Network/Device Name** field. If you change the name in the **Network/Device Name** field from readyshare to another name, the link changes accordingly.

   You can also click the link that is shown in the Link column. The fixed port is number is 21.

7. To enable password protection, select the **Admin Password Protection** check box.

8. Click the **Apply** button.

   Your settings are saved.

View and manage network folders on a USB storage device

You can view and manage network folders on a USB storage device that is attached to the USB port on an access point/router.

View network folders on a USB storage device

You can view the network folders on a USB storage device that is connected to the USB port on the access point/router.

To view network folders on a USB storage device:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

    The BASIC Home page displays.

5. Select **BASIC > ReadySHARE**.

    The USB Storage (Basic Settings) page displays.

    The Available Networks Folder table shows the following settings:

    - **Share Name**. The default share name is USB_Storage. You can click the name or you can type it in the address field of your web browser. If Not Shared is shown, the default share was deleted and no other share for the root folder exists.

    - **Read Access and Write Access**. Show the permissions and access controls on the network folder. All–no password (the default) allows all users to access the

network folder. The password for admin is the same one that you use to log in to the access point/router.

- **Folder Name**. Full path of the network folder.

- **Volume Name**. Volume name from the storage device.

- **Total Space and Free Space**. Show the current utilization of the storage device.

6. (Optional) To change the settings or add a network folder, click the **Edit** button.

   The USB Storage (Advanced Settings) page displays.

   For more information, see <u>Change a network folder on a USB storage device</u> on page 180 or <u>Add a network folder on a USB storage device</u> on page 179.

Add a network folder on a USB storage device

You can add network folders on a USB storage device connected to the USB port on the access point/router.

To add a network folder on a USB storage device:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > USB Storage > ReadySHARE**.

   The USB Storage (Advanced Settings) page displays.

6. In the Available Network Folders section, select the USB storage device.

Note: By default, the USB storage device that is connected is selected. We recommend that you do not attach more than one USB storage device the USB port (for example, through a USB hub).

7. Click the **Create Network Folder** button.

   The Create Network Folder window opens.

   If this window does not open, your web browser might be blocking pop-ups. If it is, change the browser settings to allow pop-ups.

8. From the **USB Device** menu, select the USB storage device.

   By default, the USB storage device that is connected is selected from the menu.

9. Click the **Browse** button and in the Folder field, select the folder.

10. In the **Share Name** field, type the name of the share.

11. From the **Read Access** menu and the **Write Access** menu, select the settings that you want.

   All–no password (the default) allows all users to access the network folder. The other option is that only the admin user is allowed access to the network folder. The password for admin is the same password that you use for local login to the access point/router. If you did not yet change the default password for local login, enter **admin** as the user name and **password** as the password.

12. Click the **Apply** button.

   The folder is added on the USB storage device.

13. Click the **Close Window** button.

   The window closes.

Change a network folder on a USB storage device

You can change a network folder on a USB storage device that is connected to the USB port on the access point/router.

To change a network folder on a USB storage device:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > USB Storage > ReadySHARE**.
    The USB Storage (Advanced Settings) page displays.

6. In the Available Network Folders section, select the USB storage device.

    Note: By default, the USB storage device that is connected is selected. We recommend that you do not attach more than one USB storage device the USB port (for example, through a USB hub).

7. Click the **Edit** button.
    The Edit Network Folder window opens.

8. Change the settings.

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

Router mode: Approve a USB storage device

For more security, you can set up the access point/router to share only USB storage devices that you approve.

To approve a USB storage device:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > USB Settings**.

   The USB Settings page displays.

   By default, the **Yes** radio button is selected. This setting lets you connect and access all your USB devices sequentially.

6. Select the **No** radio button.

7. Click the **Approved Devices** button.

   The USB Drive Approved Devices page displays.

8. In the Available USB Devices table, select the device that you want to approve.

9. Click the **Add** button.

   The USB device is added to the Approved USB Devices table.

10. Select the **Allow only approved devices** check box.

11. Click the **Apply** button.

    Your settings are saved.

12. To approve another USB storage device, first click the **Safely Remove USB Device** button for the currently connected USB storage device, and remove that device. For more information, see <u>Safely remove a USB storage device</u> on page 182.

    Then, connect the other USB storage device, and repeat this procedure.

Safely remove a USB storage device

Before you physically disconnect a USB storage device from the access point/router USB port, log in to the access point/router and take the USB storage device offline.

To remove a USB storage device safely:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **BASIC > ReadySHARE**.
   The USB Storage (Basic Settings) page displays.

6. In the Available Network Folders sections, select the USB storage device.

   Note: By default, the USB storage device that is connected is selected. We recommend that you do not attach more than one USB storage device the USB port (for example, through a USB hub).

7. Click the **Safely Remove USB Device** button.
   The USB storage device goes offline.

8. Physically disconnect the USB storage device.

10

Use the Access Point/Router as a Media Server

This chapter contains the following sections:

- Specify ReadyDLNA media server settings
- Play music from a storage device with iTunes server
- Set up the access point/router to work with TiVo

Specify ReadyDLNA media server settings

By default, the access point/router functions as a ReadyDLNA media server, which lets you view videos, movies, and photos on DLNA/UPnP AV-compliant media players, such as Xbox360, Playstation, and NETGEAR media players.

To specify ReadyDLNA media server settings:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > USB Storage > ReadySHARE > Media Server**.
   The Media Server (Settings) page displays.

6. Specify the settings:

   • **Enable Media Server**. By default, this check box is selected to enable the access point/router to function as a DLNA media server.

   • **Enable TiVo Support**. By default, this check box is selected to let you play ReadyNAS media on your TiVo device.

   • **Enable iTunes Server (Music Only)**. Select this check box if you want to play music from a USB device that is connected to your access point/router with iTunes on your Windows-based or Mac computer using Home Sharing. For more

information, see <u>Play music from a storage device with iTunes server</u> on page 186.

- **Media Server Name**. Click the **Click here to change the Device Name** link to change the access point/router media server name (see <u>Router mode: Change the access point/router network device name</u> on page 112).

  Note: If you change the media server device name, you can also change the LAN device name and the ReadySHARE storage folder access path. If you want to keep the access path as `\\readyshare`, do not change the media server device name.

7. To scan for new media files immediately, click the **Rescan media files** button.

   Only a shared folder with **All – no password** with **Read Access** can be scanned for media files.

   Note: The access point/router automatically scans for media files whenever new files are added to your ReadySHARE USB storage device, that is, the Content Scan **Automatic** radio button is selected.

8. Click the **Apply** button.

   Your settings are saved.

Play music from a storage device with iTunes server

iTunes server lets you play music from a USB device that is connected to the USB port on the access point/router with iTunes on your Windows-based or Mac computer or with the Apple Remote app on your iPhone or iPad. You can also use the Apple Remote app from an iPhone or iPad to play music on any AirPlay devices, such as Apple TV or AirPlay-supported receivers.

Supported music file formats are MP3, AAC, and FLAC. The maximum number of music files supported is 10,000.

Set up the access point/router's iTunes server with iTunes

You can play music from a USB device that is connected to the USB port on the access point/router with iTunes on your Windows-based computer or Mac using Home Sharing.

To set up Home Sharing, you need an Apple account and the latest version of iTunes installed on your Windows-based computer or Mac.

To set up the access point/router's iTunes server to play music on iTunes:

1. Connect a USB storage device to the USB port on the access point/router.

2. If your USB storage device uses a power supply, connect it.

   You must use the power supply when you connect the USB storage device to the access point/router.

   When you connect the USB storage device to the access point/router's USB port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers and mobile devices on the access point/router network.

3. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

5. Click the **Login** button.
   The NETGEAR Account Login page displays.

6. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

7. Select **ADVANCED > USB Storage > ReadySHARE > Media Server**.
   The Media Server (Settings) page displays.

8. Select the **Enable iTunes Server (Music Only)** check box.

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

10. On your Windows-based computer or Mac, launch iTunes.

11. Select **File > Home Sharing > Turn On Home Sharing**.
    The Home Sharing page displays.

12. Enter your Apple ID email address and password.

13. Click the **Turn On Home Sharing** button.

    When Home Sharing is enabled, a **Home Sharing** icon displays in iTunes.

14. Click the **Home Sharing** icon and from the menu, select the access point/router.

    The music that is on the USB device that is connected to the access point/router displays in iTunes.

Set up the access point/router's iTunes server with the Remote app

You can play music from a USB device that is connected to the USB port on the access point/router on your iPhone or iPad using the Apple Remote app.

To set up the access point/router's iTunes server to play music on your iPhone or iPad:

1. Connect a USB storage device to the USB port on the access point/router.

2. If your USB storage device uses a power supply, connect it.

    You must use the power supply when you connect the USB storage device to the access point/router.

    When you connect the USB storage device to the access point/router's USB port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers and mobile devices on the access point/router network.

3. Connect your iPhone or iPad to your access point/router's WiFi network.

4. Download the Remote app from the Apple App Store.

5. Launch the Remote app from your iPhone or iPad.

6. In the Remote app, click the **Add a Device** button.

    The passcode displays in the Remote app.

7. Specify the passcode in the access point/router to set up your iTunes server by doing the following:

    a. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

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

access point/router. If you do not know the IP address, see <u>Find the IP address</u> <u>of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when</u> <u>it is not connected to the Internet</u> on page 28).

c. Click the **Login** button.
The NETGEAR Account Login page displays.

d. Enter your registered email address and password and click the **LOG IN** button.
The BASIC Home page displays.

e. Select **ADVANCED > USB Storage > ReadySHARE > Media Server**.
The Media Server (Settings) page displays.

f. Select the **Enable iTunes Server (Music Only)** check box.

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

h. Enter the passcode that displays in the Remote app.

i. Click the **Allow Control** button.
Your settings are saved.
Your iPhone or iPad pairs with the access point/routerand the iTunes server is ready. The access point/router displays in the Remote app.

8. In the Remote app, tap the access point/router that your iPhone or iPad is connected to.
The music that is on the USB device that is connected to the access point/router displays in the Remote app.

Set up the access point/router to work with TiVo

You can set up your TiVo to access media files stored on a USB device that is connected to the access point/router. The TiVo must be on the same network as the access point/router. This feature supports the following file formats:

- **Video**. See and play `mpeg1`, and `mpeg2` files.

- **Music**. See and play MP3 files.

- **Pictures**. View images in `.jpg` format.

You can use the TiVo (Series 2 and later) Home Media Option to play photos and music on your Windows-based computer or Mac in your TiVo user interface.

To set up the access point/router to work with TiVo:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > USB Storage > ReadySHARE > Media Server**.
   The Media Server (Settings) page displays.

6. Make sure that the **Enable TiVo support** check box is selected.

7. If you changed the settings, click the **Apply** button.
   Your settings are saved.

11

Router Mode: Manage Dynamic DNS and FTP Access Through the Internet

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

This chapter contains the following sections:

- Router mode: Set up and manage Dynamic DNS
- Router mode: Use DDNS with FTP to access your network

For information about how to connect a USB device and specify its settings, see Share a USB Storage Device Attached to the Access Point/Router on page 166.

For information about how to use DDNS to set up a VPN tunnel, see Router Mode: Set up VPN Connections with OpenVPN on page 199.

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

Router mode: Set up and manage Dynamic DNS

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 USB storage device that is connected to your access point/router or to set up a VPN tunnel to the access point/router, 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/router to use DDNS. Then the access point/router 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/router 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.

Router mode: Set up a new Dynamic DNS account

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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Dynamic DNS**.
    The Dynamic DNS page displays.

6. Select the **Use a Dynamic DNS Service** check box.

7. From the **Service Provider** menu, select **NETGEAR**.

8. Select the **No** radio button.

9. 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**.

10. In the **Email** field, enter the email address that you want to use for your account.

11. In the **Password** field, enter the password that you want to use for your account.

    The password must contain between 6 and 32 characters.

12. Click the **Register** button.

13. Follow the onscreen instructions to register for your NETGEAR Dynamic DNS service.

Router mode: Specify a DNS account that you already created

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

To set up Dynamic DNS if you already created an account:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Dynamic DNS**.
   The Dynamic DNS page displays.

6. Select the **Use a Dynamic DNS Service** check box.

7. From the **Service Provider** menu, select your provider.

8. Select the **Yes** radio button.

9. In the **Host Name** field, enter the host name (sometimes called the domain name) for your account.

10. 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.

11. In the **Password** field, enter the password for your Dynamic DNS account.

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

13. To verify that your Dynamic DNS service is enabled in the access point/router, click the **Show Status** button.
    A message displays the Dynamic DNS status.

Router mode: Change the Dynamic DNS settings

You can change the settings for your Dynamic DNS account.

To change your settings:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

    The BASIC Home page displays.

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

    The Dynamic DNS page displays.

6. Change your DDNS account settings as necessary.

7. Click the **Apply** button.

    Your settings are saved.

Router mode: Use DDNS with FTP to access your network

You can use DDNS with FTP to access your network when you are not at the location where the access point/router is installed. To set up an FTP server that you can access through the Internet, you need a DDNS account.

Note: The access point/router supports basic DDNS only, and the login and password might not be secure. Ffor a secure connection, you can use DDNS with a VPN tunnel.

Router mode: Overview of the steps to set up an FTP server with DDNS

To set up an FTP server with DDNS:

1. Get a DDNS domain name.

    For more information, see Router mode: Set up and manage Dynamic DNS on page 192.

2. Make sure that your Internet connection is working.

    The access point/router must be in router mode and use a direct Internet connection. It cannot connect to a another router on your network to access the Internet.

3. Connect a USB storage device to the USB port of the access point/router.

4. If your USB device uses a power supply, connect it.

   You must use the power supply when you connect the USB storage device to the access point/router.

   When you connect the storage device to the access point/router, it might take up to two minutes before the storage device is ready for sharing. By default, the device is available to all devices that are connected to the access point/router network.

5. Set up FTP access on the access point/router.

   For more information, see <u>Router mode: Set up FTP access through the Internet on the access point/router</u> on page 196.

6. On a remote computer with Internet access, use FTP to access the access point/router.

   For example, is you set up a NETGEAR DDNS account, you can use ftp://*MyName*.mynetgear.com, in which *MyName* is your specific domain name.

   For more information, see <u>Router mode: Use FTP to access a storage device over the Internet</u> on page 197.

Router mode: Set up FTP access through the Internet on the access point/router

If you attach a storage device to the access point/router, you can set up FTP access through the Internet so that you can access the storage device from outside your local network, for example, when you are not at the location where the access point/router is installed.

To set up FTP access through the Internet:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > USB Storage > ReadySHARE**.
   The USB Storage (Advanced Settings) page displays.

6. Select the **FTP (via internet)** check box.
   The Link field shows the URL that you must enter from a remote device.

   Admin password protection is enabled by default.

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

8. To limit access to the admin user, do the following:

   a. In the Available Network Folders list, select a device.
      If a single device is attached to the USB port, the radio button is selected automatically.

   b. Click the **Edit** button.
      The Edit Network Folder page displays.

   c. From the **Read Access** menu, select **admin**.
      The default setting is All - no password.

   d. From the **Write Access** menu, select **admin**.
      The default setting is All - no password.

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

   f. Click the **Close Window** button.
      The pop-up window closes.

Router mode: Use FTP to access a storage device over the Internet

If you attach a USB storage device to the access point/router, before you can access the storage device through the Internet with FTP, you must first set up FTP access (see

To access a USB storage device with FTP from a remote computer to download or upload a file:

1. Take one of the following actions:

   - To download a file from a storage device connected to the access point/router, launch a web browser.
   - To upload a file to a storage device connected to the access point/router, launch an FTP client such as Filezilla.

2. Type **ftp://** and the Internet port IP address in the address field of the browser.

   For example, if your IP address is 10.1.65.4, type **ftp://10.1.65.4/shares**.

   If you are using DDNS, type the DDNS name. For example, type **ftp://**_MyName_**.mynetgear.com/shares**, in which _MyName_ is your DDNS name.

3. When prompted, enter the same credentials that you use for local login to the access point/router.

   If you did not yet change the default password for local login, enter **admin** as the user name and **password** as the password.

   The files and folders that your account can access on the storage device display. For example, you might see `share/partition1/directory1`.

4. Navigate to a location on the storage device.

5. Download or upload the file.

12

Router Mode: Set up VPN Connections with OpenVPN

If the access point/router is in router mode, you can use OpenVPN software to set up VPN connections and remotely access an office or site at which an access point/router is installed. This chapter describes how to set up OpenVPN on the access point/router and on a computer or mobile device and how to initiate a VPN connection using OpenVPN.

The chapter includes the following sections:

- Router mode: Enable and configure OpenVPN and VPN client access on the access point/router
- Router mode: Install OpenVPN client software on a remote client
- Router mode: Set up an OpenVPN connection

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

Router mode: Enable and configure OpenVPN and VPN client access on the access point/router

You must enable OpenVPN and specify the OpenVPN service settings on the access point/router before you can set up a VPN connection using OpenVPN.

Note: Make sure that remote clients install their VPN configuration files after you configure OpenVPN on the access point/router. If you make changes to the OpenVPN configuration on the access point/router, 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/router:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > VPN Service**.
   The VPN Service page displays.

6. 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.

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

   - **All sites on the Internet & Home Network**. The VPN client can access the Internet and all sites and services on the access point/router network, that is, behind the access point/router 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/router network, that is, behind the access point/router firewall, but cannot access the Internet.

   - **Auto**. The access point/router automatically uses the VPN service only for necessary access, that is, the access point/router 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.

8. Click the **Apply** button.

   Your settings are saved. OpenVPN service is enabled on theaccess point/router.

   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/router.

Router mode: Install OpenVPN client software on a remote client

To establish a VPN connection to the access point/router using OpenVPN software, a remote client must install OpenVPN client software on their computer or mobile device.

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

Router mode: Install the OpenVPN client utility and VPN configuration files on a Windows-based computer

To download and install the OpenVPN client utility and the access point/router'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. Open a web browser from the Windows-based computer, which must be connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

4. Click the **Login** button.

   The NETGEAR Account Login page displays.

5. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

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

   The VPN Service page displays.

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

   For more information, see Router mode: Enable and configure OpenVPN and VPN client access on the access point/router on page 200.

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

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

10. 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/router will fail.

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

    For more information about using OpenVPN on a Windows-based computer, visit openvpn.net/index.php/open-source/documentation/howto.html#quick.

Router mode: Install the OpenVPN client utility and VPN configuration files on a Mac

To download and install the OpenVPN client utility and the access point/router's VPN configuration files on a Mac:

1. Visit code.google.com/p/tunnelblick/, 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. Open a web browser from the Mac, which must be connected to the access point/router network.

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

4. Click the **Login** button.

    The NETGEAR Account Login page displays.

5. Enter your registered email address and password and click the **LOG IN** button.

    The BASIC Home page displays.

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

    The VPN Service page displays.

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

    For more information, see <u>Router mode: Enable and configure OpenVPN and VPN client access on the access point/router</u> on page 200.

8. In the OpenVPN configuration package download section, click the **For non-Windows** button, and download the access point/router's VPN configuration files.

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

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

    For more information about using OpenVPN on a Mac computer, visit <u>openvpn.net/index.php/access-server/docs/admin-guides/183-how-to-connect-to-access-server-from-a-mac.html</u>.

Router mode: Install the OpenVPN client utility and VPN configuration files on an iOS device

To download and install the OpenVPN client utility and the access point/router'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/router network.

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

4. Click the **Login** button.

   The NETGEAR Account Login page displays.

5. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

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

   The VPN Service page displays.

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

   For more information, see Router mode: Enable and configure OpenVPN and VPN client access on the access point/router on page 200.

8. In the OpenVPN configuration package download section, click the **For Smart Phone** button, and download the access point/router'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.

9. 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/router.

   For more information about using OpenVPN on an iOS device, visit vpngate.net/en/howto_openvpn.aspx#ios.

Router mode: Install the OpenVPN client utility and VPN configuration files on an Android device

To download and install the OpenVPN client utility and the access point/router'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/router network.

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

If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

4. Click the **Login** button.
   The NETGEAR Account Login page displays.

5. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

6. Select **ADVANCED > Advanced Setup > VPN Service**.
   The VPN Service page displays.

7. Make sure that the **Enable VPN Service** check box is selected.
   For more information, see Router mode: Enable and configure OpenVPN and VPN client access on the access point/router on page 200.

8. In the OpenVPN configuration package download section, click the **For Smart Phone** button, and download the access point/router'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.

9. On your Android device, start the OpenVPN Connect app, and search for and import the `.ovpn` file.
   Your Android device is now ready to for you to set up a VPN connection to the access point/router.
   For more information about using OpenVPN on an Android device, visit vpngate.net/en/howto_openvpn.aspx#android.

Router mode: Set up an OpenVPN connection

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/router is the gateway. To enable users to access the access point/router over a VPN connection, you must enable and configure OpenVPN service on the access point/router. 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/router** to enable a remote client such as a computer or mobile device to connect with the access point/router. (If the access point/router 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/router does not use a static WAN IP address, you can use a DDNS service for the access point/router 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/router and access the network over a VPN connection. For more information, see Router mode: Set up and manage Dynamic DNS on page 192.

Router mode: Manage VPN access to your network or Internet service at your office or home

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/router 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/router supports, see Router mode: Enable and configure OpenVPN and VPN client access on the access point/router on page 200. 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/router 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/router network at your office or home with the OpenVPN software.

The default LAN IP address scheme for the access point/router is 192.100.0.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/router IP address scheme for your office or home network (see Router mode: Manage the LAN IP address settings on page 112).

Router mode: Use a VPN tunnel to access your Internet service at your office or home

Before you leave your office or home, make sure that you set up the following:

- In addition to setting 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, allow VPN client *Internet access* through your office or home network (see Router mode: Enable and configure OpenVPN and VPN client access on the access point/router on page 200).

- Download and install OpenVPN client software on the computer or mobile device that you intend to use as a VPN client (see Router mode: Install OpenVPN client software on a remote client on page 201).

To remotely access your Internet service at your home or office:

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.

13

Manage the Advanced WiFi and Radio Features

This chapter describes how you can manage the advanced WiFi and radio features of the access point/router. For information about the basic WiFi and radio settings, see Manage the Basic WiFi and Radio Features on page 61.

Tip: If you want to change the settings of the access point/router's WiFi network, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

The chapter includes the following sections:

- Add a WiFi schedule for a radio
- Change the channel for a radio
- Change the WiFi throughput mode for a radio band
- Change the transmission output power for a radio
- Manage advanced WiFi and broadcast settings
- Manage the WPS settings
- Specify how the access point/router manages WiFi clients
- Set Up a WiFi bridge between the access/point router and another device

Add a WiFi schedule for a radio

You can use this feature to turn off the WiFi signal from a radio on the access point/router 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 a separate WiFi schedule for each WiFi band. You can also add multiple schedules for each WiFi band.

Note: You can add a WiFi schedule only if the access point/router 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/router synchronizes its clock, see Manage the time settings on page 140 and Change the NTP server on page 141.

To add a WiFi schedule for a radio:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. In the 2.4 GHz b/g/n wireless radio settings section or 5 GHz a/n/ac wireless radio settings section, click the **Add a new period** button.
   The When to turn off wireless signal page displays.

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.

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 radio for which you added the schedule.

    The radio button for the schedule lets you select the schedule if you want to change (edit) or delete it.

9. Above the table, select the **Turn off wireless signal by schedule** check box.

10. 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.

Change the channel for a radio

The available WiFi channels and frequencies depend on the region or country and the radio. The default is Auto, which enables the radio to automatically select the most suitable channel.

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 (APs), reduce interference by selecting different channels for adjacent APs. We recommend a channel spacing of four channels between adjacent APs (for example, use Channels 1 and 5, or 6 and 10).

To change the channel for one or both radios:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.

The Advanced Wireless Settings page displays.

6. From the **Channel** menu for one or each radio, select a channel.

The default is Auto, which means that the radio automatically selects the most suitable channel. When you select a particular channel, the channel selection becomes static.

7. 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 band

By default, all types of WiFi clients can access a WiFi network on the access point/router, that is, the WiFi throughput modes on the access point/router support 802.11n, 802.11g, 802.11b, 802.11ac, 802.11na, and 802.11a 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 one or both radios:

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

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

If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

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

6. From the **Mode** menu for one or each radio, select the WiFi throughput mode:

    - **2.4 GHz radio**. Select one of the following WiFi throughput modes for the 2.4 GHz radio:

      - **Up to 54 Mbps**. Legacy mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11n devices to functioning at up to 54 Mbps.

      - **Up to 145 Mbps**. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11n devices to functioning at up to 145 Mbps.

      - **Up to 300 Mbps**. Performance mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11n devices to function at up to 300 Mbps. This mode is the default mode.

      Note: WPA-PSK security supports speeds of up to 54 Mbps. Even if your devices are capable of a higher speed, WPA-PSK security limits their speed to 54 Mbps.

    - **5 GHz radio**. Select one of the following WiFi throughput modes for the 5 GHz radio:

      - **Up to 347 Mbps**. Legacy mode. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the network but limits 802.11ac and 802.11n devices to functioning at up to 347 Mbps.

      - **Up to 800 Mbps**. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the network but limits 802.11ac devices to functioning at up to 800 Mbps.

      - **Up to 1733 Mbps**. Performance mode. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the network and allows 802.11ac devices to function at up to 1733 Mbps. This mode is the default mode.

7. 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/router is set at the maximum. If two or more access point/routers 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 an access point/router. Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.

To change the transmission output power for one or both radios:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.

   The Advanced Wireless Settings page displays.

6. From the **Transmit Power Control** menu for one or each radio, select **100%**, **75%**, **50%**, or **25%**.

   The default is 100%.

7. Click the **Apply** button.

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

Manage advanced WiFi and broadcast settings

For most WiFi networks, the advanced WiFi settings work fine and you do not need to change the settings.

To manage advanced WiFi and broadcast features:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. Enter the settings as described in the following table.
   Except for the 20/40 MHz coexistence settings, the descriptions in the table (not the settings onscreen) apply to both the 2.4 GHz b/g/n wireless radio settings section and 5 GHz a/n/ac wireless radio settings section.

Setting	Description
Enable 20/40 MHz Coexistence	By default, 20/40 MHz coexistence is enabled 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 clear the **Enable 20/40 MHz Coexistence** check box to increase the WiFi speed to the maximum supported speed. The 20/40 MHz coexistence setting applies to the 2.4 GHz band only.
Fragmentation Length (256-2346)	The fragmentation length (the default is 2346), CTS/RTS threshold (the default is 2347), and the preamble mode (the default is Long Preamble) are reserved for WiFi testing and advanced configuration only.
CTS/RTS Threshold (1-2347)	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
Preamble Mode	function of the access point/router unexpectedly.

7. Click the **Apply** button.

Your settings are saved.

Manage the WPS settings

Wi-Fi Protected Setup (WPS) lets you join the WiFi network without typing the WiFi password. You can change the WPS default settings.

To manage the WPS settings:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.

   The Advanced Wireless Settings page displays.

6. Scroll down to the WPS Settings section.

   The Router's PIN field displays the fixed PIN that you use if you want to configure the access point/router's WiFi settings from another platform through WPS.

7. To disable the PIN, clear the **Enable Router's PIN** check box.

   By default, the **Enable Router's PIN** check box is selected and the access point/router's PIN is enabled. For enhanced security, you can disable the access point/router's PIN by clearing the **Enable Router's PIN** check box. However, when you disable the access point/router's PIN, WPS is not disabled because you can still use the physical **WPS** button.

   Note: The PIN function might temporarily be disabled automatically if the access point/router detects suspicious attempts to break into the access point/router's WiFi settings by using the access point/router's PIN through WPS.

8. To allow the WiFi settings to be changed automatically when you use WPS, clear the **Keep Existing Wireless Settings** check box for the 2.4 GHz band, for the 5 GHz band, or for both bands.

   By default, the **Keep Existing Wireless Settings** check boxes are selected. We recommend that you leave these check boxes selected. If you clear the check box for a band, the next time a new WiFi device uses WPS to connect to the access point/router, the access point/router WiFi settings for the band change to an automatically generated random SSID and passphrase. For information about viewing this SSID and passphrase, see Set up or change an open or secure WiFi network on page 62. Clear the **Keep Existing Wireless Settings** check box for a band *only* if you want to allow the WPS process to change the SSID and passphrase for WiFi access.

   Warning: If you clear the **Keep Existing Wireless Settings** check box for a band and use WPS to add a WiFi device to the access point/router's WiFi network, the SSID and passphrase for the band are automatically generated and other WiFi devices that are already connected to the access point/router's WiFi network might be disconnected.

9. Click the **Apply** button.

   Your settings are saved.

Specify how the access point/router manages WiFi clients

A WiFi client is any computer or mobile device that connects to the access point/router's WiFi network. The access point/router uses implicit beamforming, MU-MIMO, and airtime fairness to manage its WiFi clients. Implicit beamforming and MU-MIMO are enabled by default, but you can disable them. Airtime fairness is disabled by default, but you can enable it.

Manage Implicit Beamforming

Implicit beamforming lets the access point/router actively track clients and direct power to the access point/router antenna closest to the client. Explicit beamforming functions whether or not the client supports beamforming. Implicit beamforming means that the access point/router can use information from client devices that support beamforming to improve the WiFi signal. Implicit beamforming is enabled by default, but you can disable it.

To disable implicit beamforming:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. Scroll to the bottom of the page and clear the **Enable Implicit BEAMFORMING** check box.

7. Click the **Apply** button.

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

Manage MU-MIMO

Multiuser multiple input, multiple output (MU-MIMO) improves performance when multiple MU-MIMO-capable WiFi clients transfer data at the same time. WiFi clients must support MU-MIMO, and they must be connected to a 5 GHz WiFi band. This feature is enabled by default, but you can disable it.

To disable MU-MIMO:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.

   The Advanced Wireless Settings page displays.

6. Scroll to the bottom of the page and clear the **Enable MU-MIMO** check box.

7. Click the **Apply** button.

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

Manage Airtime Fairness

Airtime fairness ensures that all clients receive equal time on the network. Network resources are divided by time, so if five clients are connected, they each get one-fifth of the network time. The advantage of this feature is that your slowest clients do not control network responsiveness. This feature is disabled by default, but you can enable it.

To enable airtime fairness:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

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

6. Scroll to the bottom of the page and select the **Enable AIRTIME FAIRNESS** check box.

7. Click the **Apply** button.
   Your settings are saved. The radios restart and WiFi clients might need to reconnect.

Set Up a WiFi bridge between the access/point router and another device

You can use the access point/router as a WiFi bridge and connect multiple devices with WiFi, for example, at the faster 802.11ac speed. To do this, you need another WiFi router or access point (AP) in addition to the access point/router. One device is connected to the Internet over a DSL or cable modem and the other functions as a WiFi bridge.

You can connect the access point/router in router mode to the Internet modem and use the other WiFi router or AP as a WiFi bridge (assuming that the WiFi router or AP is capable of functioning as a WiFi bridge), or the other way around—connect the other WiFi router or AP to the Internet modem, and use the access point/router as a WiFi bridge.

Setting up a WiFi bridge with two access point/routers offers the following benefits:

- Take advantage of gigabit WiFi speeds on current devices.
- Use gigabit WiFi for applications such as video and gaming.
- Connect multiple devices such as a NAS, Smart TV, NeoTV, and Blu-ray player at gigabit WiFi speeds using a WiFi link.
- Avoid the need for separate WiFi adapters for each device.

For example, you could install the first access point/router in the office in which your Internet connection is located.

Then set up the second access point/router 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/router that functions as a WiFi bridge to your Smart TV, NeoTV, or Blu-ray player, and use its 802.11ac WiFi connection to the first access point/router.

The access point/router that is connected to the Internet modem does not require any special setup because the access point/router 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/router as a WiFi bridge to another access point/router, WiFi router, or AP Internet connection:

1. Make a note of the WiFi settings of the other access point/router, WiFi router, or AP that is connected to the Internet modem.

    You must know the SSID, WiFi security mode, WiFi password, and operating frequency (either 2.4 GHz or 5 GHz).

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

4. Click the **Login** button.

   The NETGEAR Account Login page displays.

5. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.

   The Advanced Wireless Settings page displays.

6. Scroll to the very bottom and select the **Use other operation mode** check box.

   The **Enable Bridge mode** radio button displays.

7. Select the **Enable Bridge mode** radio button.

   The bridge mode settings display.

8. Click the **setup bridge mode wireless settings** button.

   The Wireless Settings pop-up window opens.

9. Enter the WiFi settings of the access point/router, WiFi router, or AP that is connected to the Internet modem (that is, the *other* access point/router, WiFi router, or AP):

   a. From the **Choose a Wireless Network** menu, select the WiFi band that the other access point/router, WiFi router, or AP is using.

      For 802.11ac mode, both routers must use the same 5 GHz band.

   b. In the **Name (SSID)** field, enter the WiFi network name (SSID) that the other access point/router, WiFi router, or AP is using.

   c. In the Security Options section, select the radio button for the WiFi security that the other access point/router, WiFi router, or AP is using.

   d. If prompted, type the passphrase (the WiFi password that you must use to connect with WiFi to the other access point/router, WiFi router, or AP).

10. Click the **Apply** button.

    Your settings are saved. The pop-up window closes.

11. To change the name of the access point/router, enter a new name in the **Device Name** field.

    By default, the device name is the access point/router model (WAC124). If you use two access point/routers and you want to distinguish the name of the access point/router that you use as a WiFi bridge from the name of the access point/router that is connected to the Internet modem, you could, for example, change the name to *WiFi bridge* or something similar.

12. To let the access point/router that functions as the WiFi bridge get an IP address and DNS addresses dynamically from the access point/router. WiFi router, or AP that is connected to the Internet 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, us an IP address from the LAN IP address pool of the access point/router, WiFi router, or AP that is connected to the Internet modem. To specify a static IP address for the access point/router 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.

13. Click the **Apply** button.

    Your settings are saved. The access point/router restarts with a new IP address.

14. To reconnect, close your browser, relaunch it, and log in to the access point/router by entering **http://www.routerlogin.net**.

14

Router Mode: Manage Port Forwarding and Port Triggering

As an advanced function of the 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/router is in access point mode.

This chapter includes the following sections:

- Router mode: Manage port forwarding to a local server for services and applications
- Router mode: Manage port triggering for services and applications

Router mode: Manage port forwarding to a local server for services and applications

If the access point/router 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/router 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/router forwards all other incoming protocols (see Router mode: Set up a default DMZ server on page 76).

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

Router mode: Forward incoming traffic for a default service or application

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 Router mode: Manage reserved LAN IP addresses on page 118).

3. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

5. Click the **Login** button.

   The NETGEAR Account Login page displays.

6. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

7. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

8. Make sure that the **Port Forwarding** radio button is selected.

9. 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 <u>Router mode: Add a port forwarding rule for a custom service or application</u> on page 226).

10. In the **Internal IP Address** field, enter the IP address of the computer that must provide the service or that runs the application.

11. Click the **Add** button.

    Your settings are saved and the rule is added to the table.

Router mode: Add a port forwarding rule for a custom service or application

The access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

4. Click the **Login** button.

   The NETGEAR Account Login page displays.

5. Enter your registered email address and password and click the **LOG IN** button.

   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. Click the **Add Custom Service** button.

   The Ports - Custom Services page opens.

9. 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 dash 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 dash 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 an attached device that is listed in the table.

10. Click the **Apply** button.

Your settings are saved. The rule is added to the table on the Port Forwarding / Port Triggering page.

Router mode: Change a port forwarding rule

You can change an existing port forwarding rule.

To change a port forwarding rule:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.

    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

    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. In the table, select the radio button for the service or application name.

8. Click the **Edit Service** button.

    The Ports - Custom Services page displays.

9. Change the settings.

    For information about the settings, see Router mode: Add a port forwarding rule for a custom service or application on page 226.

10. Click the **Apply** button.

    Your settings are saved. The changed rule displays in the table on the Port Forwarding / Port Triggering page.

Router mode: Remove a port forwarding rule

You can remove a port forwarding rule that you no longer need.

To remove a port forwarding rule:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   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. In the table, select the radio button for the service or application name.

8. 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.

Router mode application example: Make a local web server public

If 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/router always assigns your web server an IP address of 192.168.0.33.

2. On the Port Forwarding / Port Triggering page, configure the access point/router to forward the HTTP service to the local address of your web server at **192.168.0.33**.

    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/router.

    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.

Router mode: How the access/point router implements a port forwarding rule

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/router.

    *   **Destination port number**. 80, which is the standard port number for a web server process.

2. The access point/router receives the message and finds your port forwarding rule for incoming port 80 traffic.

3. The access point/router changes the destination IP address in the message to, for example, 192.168.0.123 and sends the message to that computer.

4. Your web server at IP address 192.168.0.123 receives the request and sends a reply message to your access point/router.

5. Your access point/router 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.

Router mode: Manage port triggering for services and applications

If the access point/router 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/router monitors traffic to the Internet from an outbound "trigger" port that you specify. For outbound traffic from that port, the access point/router saves the IP address of the computer that sent the traffic. The access point/router 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 on page 108).

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

Router mode: Add a port triggering rule

The access point/router does not provide default services and applications for port triggering rules. You must define a custom service or application for each port triggering rule.

To add a port triggering rule:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see Find the IP address of the access point/router on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see Log in to the access point/router when it is not connected to the Internet on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
    The Port Forwarding / Port Triggering page displays.

6. Select the **Port Triggering** radio button.
    The port triggering settings display.

7. Click the **Add Service** button.
    The Port Triggering Rule page displays.

8. 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 ports.

- **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.

Router mode: Change a port triggering rule

You can change an existing port triggering rule.

To change a port triggering rule:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

    The Port Forwarding / Port Triggering page displays.

6. Select the **Port Triggering** radio button.

    The port triggering settings display.

7. In the Port Triggering Portmap Table, select the radio button for the service or application name.

8. Click the **Edit Service** button.

    The Port Triggering Rule page displays.

9. Change the settings.

    For information about the settings, see <u>Router mode: Add a port triggering rule</u> on page 232.

10. 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.

Router mode: Remove a port triggering rule

You can remove a port triggering rule that you no longer need.

To remove a port triggering rule:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

    The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

6. Select the **Port Triggering** radio button.

   The port triggering settings display.

7. In the Port Triggering Portmap Table, select the radio button for the service or application name.

8. 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.

Router mode: Specify the time-out for port triggering

The time-out period for port triggering controls how long the inbound ports stay open when the access point/router detects no activity. A time-out period is required because the access point/router cannot detect when the service or application terminates.

To specify the time-out for port triggering:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.

6. Select the **Port Triggering** radio button.

The port triggering settings display.

7. In the **Port Triggering Time-out** field, enter a value up to 9999 minutes.

   The default setting is 20 minutes.

8. Click the **Apply** button.

   Your settings are saved.

Router mode: Disable port triggering

By default, port triggering is enabled. You can disable port triggering temporarily without removing any port triggering rules.

To disable port triggering:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.

   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

6. Select the **Port Triggering** radio button.

   The port triggering settings display.

7. Select the **Disable Port Triggering** check box.

   If this check box is selected, the access point/router does not apply port triggering rules even if you specified them.

8. Click the **Apply** button.

   Your settings are saved.

Router mode application example: Port triggering for Internet Relay Chat

Some application servers, such as FTP and IRC servers, send replies to multiple port numbers. Using port triggering, you can tell the access point/router 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/router, "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/router.

3. Your access point/router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your access point/router 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/router 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/router using the NAT-assigned source port (for example, port 33333) as the destination port and also sends an "identify" message to your access point/router with destination port 113.

6. When your access point/router 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/router restores the original address information replaced by NAT and sends this reply message to your computer.

7. When your access point/router 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/router 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/router eventually senses a period of inactivity in the communications. The access point/router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

15
Diagnostics and Troubleshooting

This chapter provides information to help you diagnose and solve problems you might experience with the access point/router. 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/router from its local browser interface
- Quick tips
- Standard LED behavior when the access point/router is powered on
- Troubleshoot with the LEDs
- You cannot log in to the access point/router
- Router mode: You cannot access the Internet
- Troubleshoot Internet browsing
- Troubleshoot the WiFi connectivity
- Changes are not saved
- Troubleshoot your network using the ping utility of your computer

Reboot the access point/router from its local browser interface

You or NETGEAR technical support can reboot the access point/router from its local browser interface, either locally or remotely, for example, if the access point/router seems to be unstable or is not operating normally.

To reboot the access point/router from its local browser interface:

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

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
   The BASIC Home page displays.

5. Select **ADVANCED**.
   The ADVANCED Home page displays.

6. In the AP Information pane (in access point mode) or in the Router Information pane (in router mode), click the **Reboot** button.
   A pop-up warning window opens.

7. Click the **OK** button.
   The access point/router reboots.

Quick tips

This section describes tips for troubleshooting some common problems.

Router mode: Sequence to restart your access point/router network

If the access point/router is in router mode and you must restart your network, follow this sequence:

1. Turn off and unplug the Internet modem.

2. Turn off the access point/router.

3. Plug in the Internet modem and turn it on. Wait two minutes.

4. Turn on the access point/router 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/router is in access point mode (the default system mode), make sure that you connect the yellow Ethernet port on the access point/router 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/router and the router.

*   If the access point/router is in router mode, make sure that you connect the yellow Ethernet port on the access point/router through an Ethernet cable to a LAN port on your Internet modem.

*   For any computer or device that you connect directly through an Ethernet cable to the access point/router, make sure that you connect the Ethernet cable from the computer or device to one of the four LANs port on the access point/router.

Check the WiFi settings of your computer or mobile device

If you connect over WiFi to the access point/router, make sure that the WiFi settings on your computer or mobile device and the access point/router match exactly. The access point/router's default SSID is NETGEAR-1 and the default passphrase is sharedsecret.

Note: If you set up an access control list on the access point/router, you must add each computer or mobile device to the access control list (see Enable and manage network access control on page 81).

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/router are correct:

- **Access point mode**. If the access point/router is in access point mode (the default system mode), the LAN subnet to which your computer or device connects depends on the type of connection to the access point/router:

  - **Directly connected**. If you are directly connected over WiFi or an Ethernet cable to the access point/router 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/router. If you are using the default addressing scheme, your device's address is in the range of 192.168.0.2 to 192.168.0.254.

  - **Connected to the same network but not directly connected**. If you are not directly connected to the access point/router, 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/router is connected.

- **Router mode**. If the access point/router is in router 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/router. If you are using the default addressing scheme, your device's address is in the range of 192.168.0.2 to 192.168.0.254.

Most computers and mobile devices function as DHCP clients. If your computer or mobile device does not, enable its DHCP client so that is can obtain an IP address automatically using DHCP.

Standard LED behavior when the access point/router is powered on

After you turn on power to the access point/router, 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 USB storage device is connected to the USB of the access point/router, the USB LED is solid green.

You can use the LEDs on the top panel of the access point/router for troubleshooting.

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 you pressed the **On/Off** power button on the back of the access point/router.

- Make sure that the power adapter is securely connected to your access point/router 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 stays blinking green

When you turn on the access point/router, the Power LED lights solid green temporarily, blinks green temporarily, and finally lights solid green.

When the access point/router is upgrading firmware, the Power LED blinks green temporarily and finally lights solid green.

If the LED stays blinking green or is blinking green at any other time, this indicates a problem with the access point/router. In that situation, do the following:

- Restart the access point/router to see if the access point/router recovers.

- If the access point/router does not recover, press and hold the **Reset** button on the back to return the access point/router to its factory default settings. For more information, see Use the Reset button on page 138.

If the error persists, a hardware problem might be the cause. Contact technical support at netgear.com/support.

Access point mode: Internet LED is off

If the access point/router is in its default access point mode and the Internet LEDs is off, check the following:

- Make sure that the Ethernet cable connection is secure at the yellow WAN port (*not* a LAN port) of the access point/router and at an Ethernet port on the existing network router. In access point mode, do not connect the cable directly to an Internet modem.

- Make sure that power is turned on to the connected network router and that the network router is connected to the Internet.

- If the network router does not function as a DHCP server (this is very unusual), make sure that another DHCP server in the network is active. By default, the access point/router functions as a DHCP client and must receive an IP address from a network router or a DHCP server.

When you connect the access point/router's WAN port to the network router, use a standard straight-through Ethernet cable or an Ethernet crossover cable.

Router mode: Internet LED is off

If the access point/router is in router mode and the Internet LEDs is off, check the following:

- Make sure that you completed the initial log-in process in access point mode, that you changed the mode to router mode, and that you connected the access point/router to an Internet modem. For more information, see Use the access point/router in router mode on page 23. Only after you complete the initial log-in process in access point mode, can you change the mode to router mode.

- If the WAN type of the Internet modem is PPPoE, L2TP, or PPTP, make sure that you configured the Internet settings correctly. For more information, see Router mode: Specify a PPPoE Internet connection that uses a login on page 42 or Router mode: Specify a PPTP or L2TP Internet connection that uses a login on page 44.

- Make sure that the Ethernet cable connection is secure at the yellow WAN port (*not* a LAN port) of the access point/router and at an Ethernet port on the Internet modem.

- Make sure that power is turned on to the connected Internet modem.

When you connect the access point/router's WAN port to an Internet 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.

WiFi LED Is Off

If the WiFi LED remains off, check to see if both radios on the access point/router are disabled (see <u>Enable or disable the WiFi radios</u> on page 69). By default, both radios are enabled and the WiFi LED lights solid green or blinks green.

You cannot log in to the access point/router

If you are unable to log in to the access point/router's local browser interface from a computer or mobile device troubleshooting depends on whether the access point/router is in the default access point mode or the router mode.

Access point mode: You cannot log in to the access point/router

If the access point/router is in access point mode and you are unable to log in to its local browser interface from a computer or mobile device, check the following:

- Make sure that the computer or mobile device that you are using is connected to the access point/router or the same network as the access point/router.

- For the initial log-in process, also referred to as single sign-on (SSO), make sure that the yellow Internet port on the access point/router is connected to the Internet through an existing router in your network. The Internet LED must blink green or light solid green.

- Check the Ethernet or WiFi connection between your computer or mobile device and the access point/router:

  - **Connect over Ethernet to the same network**. If you connect the LAN port on your computer to the same network router that the access point/router is connected to, check the Ethernet cable between the computer and the LAN port on either the network router or the switch or hub that is located between the computer and the network router.

  - **Connect over Ethernet directly to the access point/router**. If you connect the LAN port on your computer directly to the access point/router, check the Ethernet cable between the computer and the LAN port on the access point/router. (Do not connect your computer to the yellow Internet port on the access point/router.)

  - **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/router. The access point/router's default SSID is NETGEAR-1 and the default passphrase is sharedsecret.

- Make sure that you are using the correct login information.
  For the initial log-in process, make sure that you log in with a MyNETGEAR account. If you do not have a MyNETGEAR account, you must create one during the initial log-in process.
  Only after you successfully completed the initial log-in process and *only if* the access point/router is not connected to the Internet, can you use the local login default user name (**admin**) and password (**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/router is connected to the Internet, you must log in with your MyNETGEAR account.

- If the access point/router'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 <u>Find the IP address of the access point/router</u> on page 29.

- Make sure that the IP address of your computer or mobile device is on the correct LAN subnet. Most computers and mobile devices function as DHCP clients. If your computer or mobile device does not, enable its DHCP client so that is can obtain an IP address automatically using DHCP. The LAN subnet to which your computer or device connects depends on the type of connection to the access point/router:

  - **Directly connected**. If you are directly connected over WiFi or an Ethernet cable to the access point/router 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/router. If you are using the default addressing scheme, your device's address is in the range of 192.168.0.2 to 192.168.0.254.

  - **Connected to the same network but not directly connected**. If you are not directly connected to the access point/router, 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/router 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/router 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.

Router mode: You cannot log in to the access point/router

If the access point/router is in router mode and you are unable to log in to its local browser interface from a computer or mobile device on the access point/router network, check the following:

- Make sure that you successfully completed the initial log-in process in access point mode before you try to log in to the access point/router in router mode.
  Only after you complete the initial log-in process in access point mode (see <u>Connect the access point/router to your existing router and log in for the first time</u> on page 17), can you change the mode to router mode and connect the access point/router to an Internet modem.

- Check the Ethernet or WiFi connection between your computer or mobile device and the access point/router:

  - **Connect over Ethernet directly to the access point/router**. If you connect the LAN port on your computer directly to the access point/router, check the Ethernet cable between the computer and the LAN port on the access point/router. (Do not connect your computer to the yellow Internet port on the access point/router.)

  - **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/router. The access point/router's default SSID is NETGEAR-1 and the default passphrase is sharedsecret.

- Make sure that you are using the correct login information.
  If the access point/router is connected to the Internet, you must log in with your MyNETGEAR account.
  Only after you successfully completed the initial log-in process and *only if* the access point/router is not connected to the Internet, can you use the local login default user name (**admin**) and password (**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 192.168.0.100).

- 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/router. If you are using the default addressing scheme, your device's address is in the range of 192.168.0.2 to 192.168.0.254. Most computers and mobile devices function as DHCP clients. If your computer or mobile device does not, enable its DHCP client so that is can obtain an IP address automatically using DHCP.

Note: Some versions of Windows and Mac OS generate and assign an IP address if a device cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the device to the access point/router 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.

Router mode: You cannot access the Internet

If the access point/router is in router mode and you can log in to the access point/router's local browser interface but cannot get an Internet connection, check if the access point/router can obtain an IP address from your Internet service provider (ISP).

Router mode: Check the Internet WAN IP address

If the access point/router is in router mode, unless your ISP provides a fixed IP address, the access point/router requests an IP address from your ISP. You can determine whether the request was successful.

To check the Internet WAN IP address:

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

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

    If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

    The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

    If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
    The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.

The BASIC Home page displays.

5. Select **ADVANCED**.

   The ADVANCED Home page displays.

6. In the Internet Port pane, click the **Connection Status** button.

   The Connection Status pop-up window opens.

   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).

7. 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/router did not obtain an IP address from your ISP.

If the access point/router cannot obtain an IP address from the ISP, you might need to force your modem to recognize the access point/router by restarting your network. For more information, see <u>Router mode: Sequence to restart your access point/router network</u> on page 241.

If the access point/router 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 <u>Router mode: Manually set up the access point/router Internet connection</u> on page 40).

- 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/router's MAC address.

  - Configure the access point/router to clone your registered computer's MAC address.

If the access point/router 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/router'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/router might not be configured as the TCP/IP gateway on your computer ore mobile device.
If your computer or mobile device obtains its information from the access point/router 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 no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**. Other browsers provide similar options.

Router mode: Check or manually start the PPPoE connection

If the access point/router 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. Open a web browser from a computer or mobile device that is connected to the access point/router network.

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

   If you are not connected to the access point/router network but to the same network as the access point/router, enter the IP address that is assigned to the access point/router. If you do not know the IP address, see <u>Find the IP address of the access point/router</u> on page 29.

   The Sign-In page displays. You are prompted to sign in with your NETGEAR account.

   If the access point/router is not connected to the Internet, you are prompted to sign in with the local login credentials (see <u>Log in to the access point/router when it is not connected to the Internet</u> on page 28).

3. Click the **Login** button.
   The NETGEAR Account Login page displays.

4. Enter your registered email address and password and click the **LOG IN** button.
    The BASIC Home page displays.

5. Select **ADVANCED**.
    The ADVANCED Home page displays.

6. In the Internet Port pane, click the **Connection Status** button.
    The Connection Status pop-up window opens.

7. Check the information to see if your PPPoE connection is up and working.
    If the access point/router is not connected, click the **Connect** button.
    The access point/router continues to attempt to connect indefinitely.

8. If you cannot connect after several minutes, the access point/router 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/router does not authenticate
    using PPPoE until data is transmitted to the network.

Troubleshoot Internet browsing

If the access point/router 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/router is in router mode and you can log in to the access
    point/router's local browser interface but you cannot get an Internet connection,
    check if the access point/router can obtain an IP address from your ISP (see)

*   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 Router mode: Unblock the traffic meter
    after the traffic limit is reached on page 160). 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/router'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/router is in router mode, the access point/router 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/router 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 no longer need to run that software after installing the access point/router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select the **Never dial a connection**. Other browsers provide similar options.

Troubleshoot the WiFi connectivity

If you are experiencing trouble connecting over WiFi to the access point/router, try to isolate the problem:

- Make sure that the WiFi settings in your WiFi device and access point/router match exactly.
For a device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the access point/router and WiFi device must match exactly. The default SSID is NETGEAR-1 and default WiFi pasphrase is sharedsecret. This information is also on the access point/router label (see Access point/router label on page 14).

- Does the WiFi device that you are using find your WiFi network?
If not, check the WiFi LED on the top of the access point/router. If the WiFi LED is off, both WiFi radios are probably off too. For more information about the WiFi radios, see Enable or disable the WiFi radios on page 69.

- If you disabled the access point/router'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 68.

- Does your WiFi device support the security that you are using for your WiFi network (WPA or WPA2)? For information about changing the WiFi security, see Set up or change an open or secure WiFi network on page 62.

  Tip: If you want to change the WiFi settings of the access point/router'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/router too far from your WiFi device or too close? Place your WiFi device near the access point/router but at least 6 feet (1.8 meters) away and see whether the signal strength improves.

- Are objects between the access point/router and your WiFi device blocking the WiFi signal? For more information, see <u>Position the access point/router</u> on page 262.

Changes are not saved

If the access point/router does not save the changes that you make through the local browser interface, do the following:

- When entering configuration settings, always click the **Apply** button before moving to another page or tab, or your changes are lost.

- Click the **Refresh** button in the local browser interface. 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

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 easily troubleshoot a network using the ping utility in your computer.

Test the LAN path from your computer to the access point/router

You can ping the access point/router from your computer to verify that the LAN path to your access point/router is set up correctly. You can do this whether the access point/router is in access point mode or in router mode.

To ping the access point/router 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/router, 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, one of the following problems might be present:

- Wrong physical connections
  Make sure that the LAN port on your computer is connected to a LAN port on the access point/router.
  If the access point/router 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 your computer and router.

- Wrong network configuration
  Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
  Verify that the IP addresses and LAN subnet for the access point/router and your computer are correct. For more information, see <u>Check the DHCP network settings of your computer or mobile device</u> on page 242.

Router mode: Test the path from your computer to a remote device

If the access point/router is in router mode, to test the path from a Windows-based computer that is connected to the access point/router 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 <u>Test the LAN path from your computer to the access point/router</u> on page 253.

3. If you do not receive replies, check the following:

- Check to see that IP address of the access point/router 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/router 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 Internet 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 Router mode: Manually set up the access point/router Internet connection on page 40).

- 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 broadband 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/router to the factory default settings, which are shown in the following table.

For more information about resetting the access point/router to its factory settings, see

Table 3. WAC124 access point/router factory default settings

Feature	Default Setting
Login to the local browser interface	
Login URL	www.routerlogin.net (if the access point/router does not get an IP address from a DHCP server, the IP address is 192.168.0.100)
SSO login	MyNETGEAR registered email address and password The initial log-in requires SSO and a MyNETGEAR account.
Local login user name	admin (case-sensitive, nonconfigurable) This user name applies only *after* initial configuration and if the access point/router is not connected to the Internet.
Local login password	password (case-sensitive, configurable) This password applies only *after* initial configuration and if the access point/router is not connected to the Internet.
System modes	
Access point mode	Enabled by default
Router mode	Disabled by default. Only after you complete the initial log-in process in access point mode, can you change the mode to router mode and connect the access point/router to an Internet modem.
DHCP settings	
DHCP client	Enabled (LAN client in access point mode. WAN client in router mode.)
DHCP server	Enabled in router mode (does not apply to access point mode)
WiFi network	
WiFi communication	Enabled for Wireless 1 network Disabled for Wireless 2 and Wireless 3 networks
SSID names	Wireless 1 default network: NETGEAR-1 Wireless 2 optional network: NETGEAR-2 Wireless 3 optional network: NETGEAR-3

Table 3. WAC124 access point/router factory default settings (Continued)

Feature	Default Setting
Security for Wireless 1 default network	WPA2-PSK [AES] mode The default WiFi passphrase is sharedsecret. This information is also on the access point/router label.
Country/region	North America: United States Europe: Europe Other continents: Varies by region
Channel	Auto. The available channels depend on the region.
WiFi throughput mode	Up to 300 Mbps at 2.4 GHz Up to 1733 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
20/40 MHz coexistence	Enabled
Fragmentation length	2346
CTS/RTS threshold	2347
Preamble mode	Long Preamble
Radio transmission power	100%
Implicit beamforming	Enabled
MU-MIMO	Enabled
Airtime Fairness	Disabled
Bridge mode	Disabled
WPS	
WPS capability	Enabled
Router's PIN	Enabled. For more information, see Manage the WPS settings on page 216.
Keep Existing Wireless Settings	Enabled
QoS	
Internet access QoS	Disabled
802.11e WMM	Enabled
UPnP	Enabled

Table 3. WAC124 access point/router 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)
NAT filtering	Secure (does not apply to access point mode)
SIP ALG	Enabled in router mode (does not apply to access point mode)
IGMP proxying	Disabled in router mode (does not apply to access point mode)
IPSec Passthrough	Enabled in router mode (does not apply to access point mode)
PPTP Passthrough	Enabled in router mode (does not apply to access point mode)
L2TP Passthrough	Enabled in router mode (does not apply to access point mode)
Remote management	Disabled in router mode (does not apply to access point mode)

Technical specifications

The following table shows the technical specifications of the access point/router. For more information, see the product data sheet, which you can download by visiting netgear.com/support/download/.

Table 4. Specifications of the WAC124 access point/router

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 5.94 x 2.14 in. (235.51 x 150.76 x 54.5 mm)

Table 4. Specifications of the WAC124 access point/router (Continued)

Feature	Description
Weight	0.831 lb (377 g)
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	10 to 90% maximum relative humidity, noncondensing
Storage temperature	–20° to 70°F (–4° to 158°C)
Storage humidity	5 to 95% maximum relative humidity, noncondensing
LAN	Four 10/100/1000BASE-T Ethernet (RJ-45) ports with Auto Uplink (Auto MDI-X)
WAN (Internet)	One 10/100/1000BASE-T Ethernet (RJ-45) port with Auto Uplink (Auto MDI-X)
USB	One USB 2.0 port to connect a USB storage device or printer
WiFi standards	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 300 Mbps at 2.4 GHz Up to 1733 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/router can support a maximum of 64 WiFi clients: Maximum number of 2.4 GHz WiFi clients: 32 Maximum number of 5 GHz WiFi clients: 32 In a WiFi network, the number of clients is 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 Japan: 2.412–2.472 GHz
Operating frequency range 5 GHz band	US: 5.180–5.240 + 5.745–5.825 GHz Europe: 5.180–5.240 GHz Australia: 5.180–5.240 + 5.745–5.825 GHz Japan: 5.180–5.240 GHz
802.11 security	WPA2-PSK, WPA and WPA2 (mixed mode), and WPA/WPA2 Enterprise
Safety Certification	CE (EN60950)

B

Position and Wall-Mount the Access Point/Router

This appendix includes the following sections:

- <u>Position the access point/router</u>
- <u>Wall-mount the access point/router</u>

Position the access point/router

Before you install the access point/router, consider how you will position the access point/router.

The access point/router 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/router. 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/router'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/router according to the following guidelines:

- Place your access point/router 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/router is within reach of an AC power outlet.

- Place the access point/router in an elevated location, minimizing the number walls and ceilings between the access point/router and your other devices.

- Place the access point/router 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/router 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 <u>Change the channel for a radio</u> on page 211).

Wall-mount the access point/router

Wall-mounting holes are on the bottom of the access point/router. The distance between the holes is 4.13 in. (105 mm).

We recommend that you use pan head Phillips wood screws, No. 6 type screw, 1 inch long (U.S.) or 3.5 x 20 mm (diameter x length, European).

To wall-mount the access point/router:

1. Drill holes in the wall where you want to wall-mount the access point/router.

   The distance between the holes in the wall must be 4.13 in. (105 mm).

2. Insert wall anchors in the holes.

3. Insert screws into the wall anchors, leaving 3/16 in (0.5 cm) of each screw exposed.

4. Align the access point/router's wall-mounting holes with the screws and mount the access point/router so that the antennas are at the top.