NETGEAR®

User Manual

Nighthawk Pro Gaming Router

Model XR500

May 2022
202-11808-05

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

Support and Community

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

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

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

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

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

Do not use this device outdoors.

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

Trademarks

Contents

Chapter 7 Manage the Router's Network Settings

Chapter 8 Manage the Router's WiFi Settings

Chapter 9 Maintain the Router

Chapter 10 Share USB Storage Devices Attached to the Router

Chapter 15 Use VPN to Access An External Network

Chapter 16 Manage and Customize Internet Traffic Rules for Ports

Chapter 17 Troubleshooting

Appendix A Supplemental Information

1

Hardware Setup

This user manual is for the NETGEAR Nighthawk® Pro Gaming Router.

This chapter contains the following sections:

- Unpack your router
- LEDs, buttons, and borts on the front panel, top panel, and left side panel
- Rear panel
- Attach the antennas
- Router Label
- Position your router
- Cable your router
- Turn the LEDs on or off using the LED On/Off switch

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

Unpack your router

Your package contains the Nighthawk Pro Gaming Router, the four antennas, the power adapter, and an Ethernet cable.

Figure 1. Package contents

LEDs, buttons, and borts on the front panel, top panel, and left side panel

The status LEDs are located on the front panel, two buttons with LEDs are located on the top panel, and two USB 3.0 ports are located on the left side panel of the router

Figure 2. Front view

Table 1. LED descriptions

LED and Button	Description
Power LED	**Solid amber**. The router is starting. **Blinking amber**. The firmware is upgrading, or the **Reset** button was pressed. **Solid white**. The router is ready. **Solid amber**. The firmware is corrupted. **Off**. Power is not supplied to the router
Internet LED Internet	**Solid white**. The Internet connection is ready. **Solid amber**. The router detected an Ethernet cable connection to the modem. **Off**. No Ethernet cable is connected between the router and the modem.

Table 1. LED descriptions (Continued)

LED and Button	Description
2.4 GHz WiFi LED 2.4 GHz	**Solid white**. The 2.4 GHz WiFi radio is operating. **Blinking white**. The router is sending or receiving WiFi traffic. **Off**. The 2.4 GHz WiFi radio is off.
5 GHz WiFi LED 5 GHz	**Solid white**. The 5 GHz WiFi radio is operating. **Blinking white**. The router is sending or receiving WiFi traffic. **Off**. The 5 GHz WiFi radio is off.
Guest WiFi LED Guest WiFi	**Solid white**. The guest WiFi network is operating. **Blinking white**. The router is sending or receiving WiFi traffic. **Off**. The guest WiFi radio is off in both the 2.4 GHz band and the 5 GHz band.
USB 3.0 port 1 LED and USB 3.0 port 2 LED USB1 USB2	**Solid white**. A USB device is connected and is ready. **Blinking white**. A USB device is plugged in and is trying to connect. **Off**. No USB device is connected, or someone clicked the **Safely Remove Hardware** button and it is now safe to remove the attached USB device.
Ethernet LEDs for ports 1–4 Eth 1 Eth 2 Eth 3 Eth 4	The LED color indicates the speed: white for Gigabit Ethernet connections and amber for 100 Mbps or 10 Mbps Ethernet connections. **Solid white**. The router detected a 1 Gbps link with a powered-on device. **Blinking white**. The port is sending or receiving traffic at 1 Gbps. **Solid amber**. The router detected a 100 Mbps or 10 Mbps link with a powered-on device. **Blinking amber**. The port is sending or receiving traffic at 100 Mbps or 10 Mbps. **Off**. No device is connected to this Ethernet port.
WiFi/On/Off button and LED	Pressing this button for two seconds turns the 2.4 GHz and 5 GHz WiFi radios on and off. If this LED is lit, the WiFi radios are on. If this LED is off, the WiFi radios are turned off and you cannot use WiFi to connect to the router
WPS button and LED	This button lets you use WPS to join the WiFi network without typing the WiFi password. The WPS LED blinks white during this process and then lights solid white.

Note: If the **LED On/Off** switch on the rear panel is moved to the Off position, all the LEDs except the **Power** LED are turned off.

Rear panel

The following figure shows the rear panel connectors and buttons.

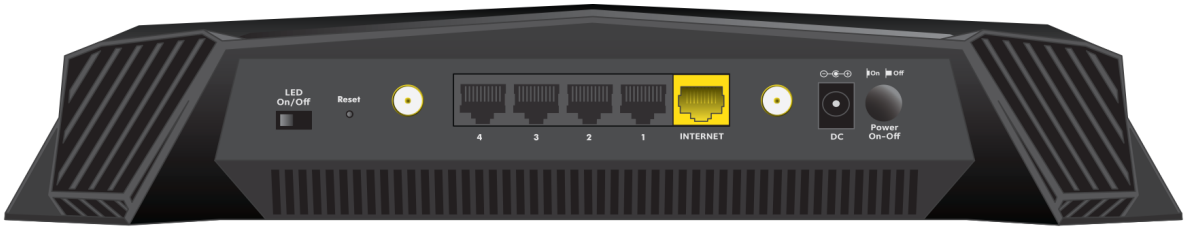


Figure 3. Rear panel

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

- **LED On/Off switch**. If this switch is in the Off position, all the router's LEDs, including the LEDs on the four active antennas, but not the Power LED, are turned off.
- **Reset button**. Pressing the **Reset** button resets the router.
  If you press the **Reset** button for up to 30 seconds or until the Power LED starts blinking amber, the router returns to its factory settings. For information about the factory settings, see Factory settings on page 211.
- **One antenna connector**.
- **Ethernet ports**. Four Gigabit Ethernet RJ-45 LAN ports named Eth4 to Eth1. Use these ports to connect the router to LAN devices.
- **Internet port**. One yellow Gigabit Ethernet RJ-45 WAN port to connect the router to an Internet modem such as a cable modem or DSL modem.
- **One antenna connector**.
- **DC power connector**. Connect the power adapter that came in the product package to the DC power connector.
- **Power On/Off button**. Press the **Power On/Off** button to provide power to the router.

Attach the antennas

The router comes with four antennas. Attach two antennas to the rear panel and attach one antenna to each side panel.

Figure 4. Attach the antennas and position them for best WiFi performance

To attach the antennas:

1. Align the antennas with the antenna posts on the router.
2. Attach the antennas on the threaded antenna posts.
3. Position the antennas for the best WiFi performance.

   We recommend that you position all of the antennas as shown in the previous figure. Position the antennas on the rear panel vertically and position the antennas on the side panels at a 45 degree angle.

Router Label

The router label on the top panel of the router shows the login information, WiFi Network Name (SSID), network key (password), serial number, and MAC address.

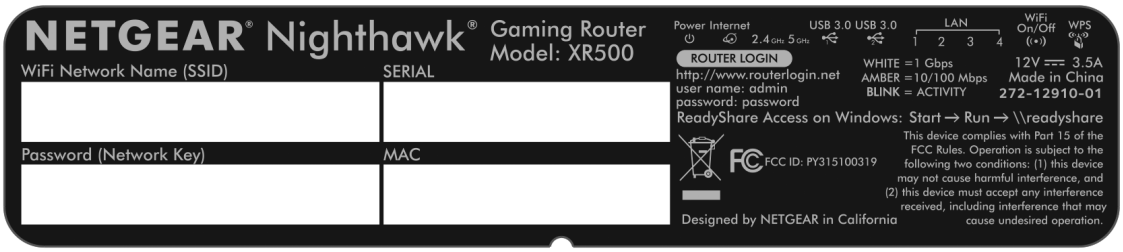


Figure 5. Router label

Figure 6. Location of the router label

Position your router

The 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 router.

To take full advantage of the 11ad advanced feature, your router must be placed within 20 feet and within line of sight of the 11ad enabled device that you are connecting to it.

In addition, position your router according to the following guidelines:

- Place your router near the center of the area where your computers and other devices operate, and within line of sight to your WiFi devices.
- Make sure that the router is within reach of an AC power outlet and near Ethernet cables for wired computers.
- Place the router in an elevated location, minimizing the number walls and ceilings between the router and your other devices.
- Place the router away from electrical devices such as these:
  - Ceiling fans
  - Home security systems
  - Microwaves
  - Computers
  - Base of a cordless phone
  - 2.4 GHz cordless phone
  - 5 GHz cordless phone
- Place the 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

The following factors might limit the range of your WiFi:

- The thickness and number of walls the WiFi signal passes through.
- Other WiFi access points in and around your home might affect your router's signal. WiFi access points are routers, repeaters, WiFi range extenders, and any other device that emits a WiFi signal for network access.

Cable your router

Power on your router and connect it to a modem.

Figure 7. Cable your router

To cable your router:

1. Unplug your modem, remove and reinsert the backup battery if it uses one, and then plug the modem back in.
2. Use the Ethernet cable to connect the modem to the yellow Internet port on the router.

   Note: If your Internet connection does not require a modem, connect your main Ethernet cable to the yellow Internet port on the router.

3. Connect the power adapter to your router and plug the power adapter into an outlet.
4. Press the **Power On/Off** button on the rear panel of the router.
   The router's Power LED lights solid white when the router is ready.

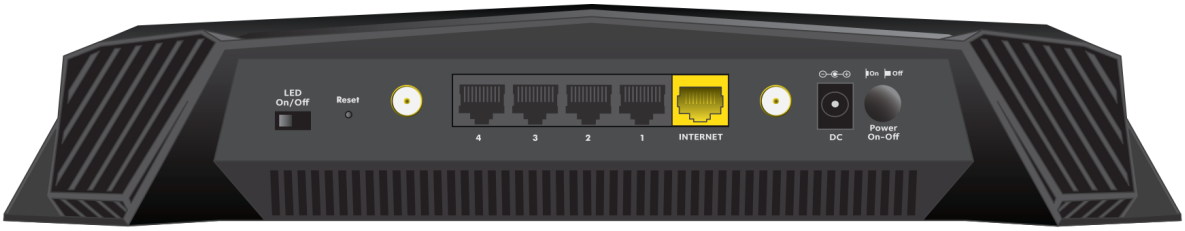
Turn the LEDs on or off using the LED On/Off switch

You can turn off the router LEDs using the **LED On/Off** switch on the rear panel of the router. Note that the Power LED stays lit even if the **LED On/Off** switch is in the Off position.

Note: You can also log in to the router to disable or enable LED blinking or turn off the LEDs (see Disable or enable LED blinking or turn off LEDs on page 138).

To turn the LEDs on or off using the LED On/Off switch:

Move the **LED On/Off** switch on the rear panel to the On or Off position.



2

Connect to the Network and Access the Router

You can connect to the router's WiFi networks or use a wired Ethernet connection. This chapter describes the ways you can connect and how to access the router and log in.

The chapter contains the following sections:

Connect to the router network

You can connect to the router network using a wired, WiFi, or WPS connection.

Note: If you set up your computer to use a static IP address, change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Connect to the router using a wired connection

You can connect your computer to the router using an Ethernet cable and join the router's local area network (LAN).

To connect your computer to the router with an Ethernet cable:

1. Make sure that the router is receiving power (its Power LED is lit).
2. Connect an Ethernet cable to an Ethernet port on your computer.
3. Connect the other end of the Ethernet cable to an Ethernet port on the router.
   Your computer connects to the local area network (LAN).

Connect to the router WiFi network

You can connect WiFi-enabled devices to the router WiFi network using the router WiFi network name and password.

To connect to the WiFi network:

1. Make sure that the router is receiving power (its Power LED is lit).
2. On your WiFi-enabled device, open your device's WiFi network management settings.
3. Find and select the router WiFi network name (SSID).
   The router WiFi network name (SSID) is on the router label.
4. Enter the router network key (password).
   The router network key (password) is on the router label.
   Your device connects to the WiFi network.

WiFi connection using WPS

You can connect to the router's WiFi network with Wi-Fi Protected Setup (WPS) or you can find and select the WiFi network.

To use WPS to connect to the WiFi network:

1. Make sure that the router is receiving power (its Power LED is lit).
2. Check the WPS instructions for your computer or mobile device.
3. Press the **WPS** button on the router.
4. Within two minutes, on your computer or mobile device, press its **WPS** button or follow its instructions for WPS connections.

   Your computer or mobile device connects to the WiFi network.

Types of logins

Separate types of logins serve different purposes. It is important that you understand the difference so that you know which login to use when.

Several types of logins are associated with the router:

- **ISP login**. The login that your ISP gave you logs you in to your Internet service. Your service provider gave you this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **WiFi network key or password**. Your router is preset with a unique WiFi network name (SSID) and password for WiFi access. This information is on the router label.
- **Router login**. This logs you in to the router web interface from a web browser as admin.

Use a web browser to access the router

When you connect to the network (either with WiFi or with an Ethernet cable), you can use a web browser to access the router to view or change its settings. When you access the router, the software automatically checks to see if your router can connect to your Internet service.

Automatic Internet setup

You can set up your router automatically, or you can use a web browser to access the router and set up your router manually. Before you start the setup process, get your ISP information and make sure that the computers and devices in the network are using the settings described here.

When your Internet service starts, your Internet service provider (ISP) typically gives you all the information needed to connect to the Internet. For DSL service, you might need the following information to set up your router:

- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address setting (special deployment by ISP; this setting is rare)

If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP login program on your computer to access the Internet. When you start an Internet application, your router automatically logs you in.

Note: During the setup process with the installation assistant, after you are connected to the Internet, you are prompted to register your product with NETGEAR. If you already have a NETGEAR account, you can use your existing account. If you do not yet have a free NETGEAR account, you can create one.

The NETGEAR installation assistant runs on any device with a web browser.

To automatically set up your router:

1. Make sure that the router is powered on.
2. Make sure that your computer or mobile device is connected to the router with an Ethernet cable (wired) or over WiFi with the preset security settings listed on the label.

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

3. Launch a web browser.

   The page that displays depends on whether you accessed the router before:

   - The first time you set up the Internet connection for your router, the browser goes to **http://www.routerlogin.net** and the Configuring the Internet Connection page displays.
   - If you already set up the Internet connection, enter **http://www.routerlogin.net** in the address field for your browser to start the installation process.

4. Follow the instructions on the page.

   The router connects to the Internet.

Note: During the setup process, you are required to change the default router password. The ideal secure password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. The password can be up to 30 characters.

5. If the browser does not display a router page, do the following:
   - Make sure that the computer is connected to one of the LAN Ethernet ports or over WiFi to the router.
   - Make sure that the router is receiving power and that its Power LED is lit.
   - Close and reopen the browser or clear the browser cache.
   - Browse to **http://www.routerlogin.net**.
   - If the computer is set to a static or fixed IP address (this setting is uncommon), change it to obtain an IP address automatically from the router.
6. If the router does not connect to the Internet, do the following:
   a. Review your settings. Make sure that you selected the correct options and typed everything correctly.
   b. Contact your ISP to verify that you are using the correct configuration information.
   c. Read You cannot access the Internet on page 203. If problems persist, register your NETGEAR product and contact NETGEAR Technical Support.

After the router connects to the Internet, you are prompted to register your product with NETGEAR. If you already have a NETGEAR account, you can use your existing account. If you do not yet have a free NETGEAR account, you can create one.

After successful installation and registration, you are prompted to download the free Nighthawk app, which you can install on your mobile device.

Log in to the router

After you automatically set up your router (see Automatic Internet setup on page 22), the next time that you connect to your router and launch a web browser, the browser automatically displays the router web interface. If you want to view or change settings for the router later, you can use a browser to log in to the router web interface.

To log in to the router:

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

   Note: You can also enter **http://www.routerlogin.com** or **http://192.168.1.1**. The procedures in this manual use **http://www.routerlogin.net**.

A login window opens.

3. Enter the router admin user name and password.
   The router admin user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays. By default, the Dashboard shows the following panes:

   - Internet Status
   - Wireless Status
   - Guest Wireless Status
   - Network Overview
   - CPU Usage
   - Installed R-Apps

   For information about these panes, see View router system information on page 68.

   For information about how you can change the panes that are shown on the Dashboard, see Customize the dashboard on page 69.

Change the language

By default, the language is set to **Auto**.

To change the language:

1. Launch a web browser from a computer or mobile device that is connected to the network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

   The Dashboard displays.
4. In the upper right corner, click the **globe** icon and select a language from the **Language** menu.
   The page refreshes with the language that you selected.

Manage your router with the NETGEAR Nighthawk app

With the NETGEAR Nighthawk app, you can easily manage your router. With the app, you can update your router's firmware, change your WiFi network settings, register your router with NETGEAR, and more.

The Nighthawk app is available for iOS and Android mobile devices.

To manage your router using the Nighthawk app:

1. To download the app, visit https://www.netgear.com/home/apps-services/nighthawk-app/default.aspx.
2. On your mobile device, tap **Settings > Wi-Fi** and find and connect to your router's WiFi network.

   Your router's WiFi network name (SSID) and network key (password) are on the router label.
3. Launch the Nighthawk app on your mobile device.

   The dashboard displays.
4. Tap a feature on the dashboard to view or change the settings.

3

Specify Your Internet Settings

Usually, the quickest way to set up the router to use your Internet connection is to allow the installation assistant to detect the Internet connection when you first access the router with a web browser (see Automatic Internet setup on page 22). You can also customize or specify your Internet settings.

This chapter contains the following sections:

Use the Internet Setup Wizard

You can use the Setup Wizard to detect your Internet settings and automatically set up your router. The Setup Wizard is not the same as the pages that display the first time you connect to your router to set it up.

To use the Setup Wizard:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > Setup Wizard**.
   The Setup Wizard page displays.
5. Select the **Yes** radio button.
   If you select the **No** radio button, after you click the **Next** button, you are taken to the Internet Setup page (see Manually set up the Internet connection on page 28).
6. Click the **Next** button.
   The Setup Wizard searches your Internet connection for servers and protocols to determine your Internet configuration.

Manually set up the Internet connection

You can view or change the router's Internet connection settings.

Specify an Internet connection without a login

To specify the Internet connection settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Settings > Setup > Internet Setup**.

   The Internet Setup page displays.

5. In the Does your Internet connection require a login? section, leave the **No** radio button selected.
6. If your Internet connection requires an account name or host name, click the **Edit** button in the Account Name section and enter the account name.
7. If your Internet connection requires a domain name, type it in the **Domain Name (If Required)** field.

   For the other sections on this page, the default settings usually work, but you can change them.

8. Select an Internet IP Address radio button:

   - **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
   - **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP router to which your router connects.

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

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

10. Select a Router MAC Address radio button:

    - **Use Default Address**. Use the default MAC address.
    - **Use Computer MAC Address**. The router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
    - **Use This MAC Address**. Enter the MAC address that you want to use.

11. Click the **Apply** button.

    Your settings are saved.

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

    If the NETGEAR website does not display within one minute, see You cannot access the Internet on page 203.

Specify an Internet connection that uses a login

To view or change the basic Internet setup:

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Setup > Internet Setup**.

   The Internet Setup page displays.
5. In the Does your Internet connection require a login? section, select the **Yes** radio button.
6. From the **Internet Service Provider** menu, select the encapsulation method: **PPPoE**, **L2TP**, or **PPTP**.
7. In the **Login** field, enter the login name that your ISP gave you.

   This login name is often an email address.
8. In the **Password** field, type the password that you use to log in to your Internet service.
9. If your ISP requires a service name, type it in the **Service Name (if Required)** field.
10. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.
11. To change the number of minutes until the Internet login times out, in the **Idle Timeout (In minutes)** field, type the number of minutes.

    This period 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.
12. Select an Internet IP Address radio button:

- **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP router to which your router connects.

13. Select a Domain Name Server (DNS) Address radio button:
    - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
    - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
14. Select a Router MAC Address radio button:
    - **Use Default Address**. Use the default MAC address.
    - **Use Computer MAC Address**. The router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
    - **Use This MAC Address**. Enter the MAC address that you want to use.
15. Click the **Apply** button.
    Your settings are saved.
16. Click the **Test** button to test your Internet connection.
    If the NETGEAR website does not display within one minute, see You cannot access the Internet on page 203.

Specify IPv6 Internet connections

You can set up an IPv6 Internet connection if the router does not detect it automatically.

To set up an IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.

4. Select **Settings > Advanced Settings > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select the IPv6 connection type:

   - If you are not sure, select **Auto Detect** so that the router detects the IPv6 type that is in use.
     For more information, see Use Auto Detect for an IPv6 Internet connection on page 33.
   - If your Internet connection does not use PPPoE or DHCP, or is not fixed, but is IPv6, select **Auto Config**.
     For more information, see Use Auto Config for an IPv6 Internet connection on page 34.

   For information about the other IPv6 connection types that the router supports, see the following sections:

   - Set up an IPv6 6to4 tunnel Internet connection on page 35
   - Set up an IPv6 6rd Internet connection on page 37
   - Set up an IPv6 pass through Internet connection on page 39
   - Set up an IPv6 fixed Internet connection on page 39
   - Set up an IPv6 DHCP Internet connection on page 41
   - Set up an IPv6 PPPoE Internet connection on page 42

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

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

Use Auto Detect for an IPv6 Internet connection

To set up an IPv6 Internet connection through autodetection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Detect**.
   The page adjusts.
   The 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 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 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.
6. 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 router assigns IPv6 addresses to the devices on your home network (the LAN).
7. (Optional) Select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.
   If you do not specify an ID here, the router generates one automatically from its MAC address.

8. Select an IPv6 Filtering radio button:
   - **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
   - **Open**. In open mode, the router inspects UDP packets only.
9. Click the **Apply** button.
   Your settings are saved.

Use Auto Config for an IPv6 Internet connection

To set up an IPv6 Internet connection through autoconfiguration:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Setting > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Config**.
   The page adjusts.
   The 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 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 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.
6. (Optional) In the **DHCP User Class (If Required)** field, enter a host name.
   Most people can leave this field blank, but if your ISP gave you a specific host name, enter it here.

7. (Optional) In the **DHCP Domain Name (If Required)** field, enter a domain name.

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

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

   - **Get Automatically from ISP**. This is the default setting. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
   - **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. 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 router assigns IPv6 addresses to the devices on your home network (the LAN).

10. (Optional) Select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

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

11. Select an IPv6 Filtering radio button:

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

12. Click the **Apply** button.

    Your settings are saved.

Set up an IPv6 6to4 tunnel Internet connection

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

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **6to4 Tunnel**.
   The page adjusts.
   The 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 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.
6. Select a Remote 6to4 Relay Router radio button:
   - **Auto**. Your 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.
7. Select an IPv6 Domain Name Server (DNS) Address radio button:
   - **Get Automatically from ISP**. This is the default setting. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
   - **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. 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 router assigns IPv6 addresses to the devices on your home network (the LAN).

9. Select an IPv6 Filtering radio button:
   - **Secured**. In secured mode, which is the default mode, the router inspects both TCP and UDP packets.
   - **Open**. In open mode, the router inspects UDP packets only.
10. (Optional) Select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

    If you do not specify an ID here, the router generates one automatically from its MAC address.
11. Click the **Apply** button.

    Your settings are saved.

Set up an IPv6 6rd Internet connection

The 6rd protocol makes it possible to deploy IPv6 to sites by using a service provider's IPv4 network. 6rd 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.

To set up an IPv6 6rd Internet connection:

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > IPv6**.

   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **6rd**.

The page adjusts.

The router automatically detects the information in the following sections:

- **6rd (IPv6 Rapid Development) Configuration**. The 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 router, the page adjusts to display the correct settings in this section.
- **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the 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.

6. Specify the following 6rd settings:
   - **6rd Prefix**. Enter the IPv6 prefix that your ISP gave you.
   - **6rd Prefix Length**. Enter the IPv6 prefix length that your ISP gave you.
   - **6rd IPv4 Border Relay Address**. Enter the border router's IPv4 address that your ISP gave you.
   - **6rd IPv4 Address Mask Length**. Enter the IPv4 mask length that your ISP gave you.
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 this address.
   - **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. 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 router assigns IPv6 addresses to the devices on your home network (the LAN).
9. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the router's LAN interface.

   If you do not specify an ID here, the router generates one automatically from its MAC address.
10. Select an IPv6 Filtering radio button:

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

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

Set up an IPv6 pass through 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 router does not process any IPv6 header packets.

To set up a pass-through IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Pass Through**.
   The page adjusts, but no additional fields display.
6. Click the **Apply** button.
   Your settings are saved.

Set up an IPv6 fixed Internet connection

To set up a fixed IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Settings > Advanced Settings > IPv6**.

   The IPv6 page displays.

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

   The page adjusts.

6. In the WAN Setup section, configure the fixed IPv6 addresses for the WAN connection:

   - **IPv6 Address/Prefix Length**. The IPv6 address and prefix length of the router WAN interface.
   - **Default IPv6 Gateway**. The IPv6 address of the default IPv6 gateway for the router's WAN interface.
   - **Primary DNS Server**. The primary DNS server that resolves IPv6 domain name records for the router.
   - **Secondary DNS Server**. The secondary DNS server that resolves IPv6 domain name records for the router.

   Note: If you do not specify the DNS servers, the router uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup page (see Manually set up the Internet connection on page 28).

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

8. In the **IPv6 Address/Prefix Length** fields, specify the static IPv6 address and prefix length of the router's LAN interface.

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

9. Select an IPv6 Filtering radio button:

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

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

Set up an IPv6 DHCP Internet connection

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **DHCP**.
   The page adjusts.
   The 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 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 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.
6. (Optional) In the **User Class (If Required)** field, enter a host name.
   Most people can leave this field blank, but if your ISP gave you a specific host name, enter it here.
7. (Optional) In the **Domain Name (If Required)** field, enter a domain name.

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

8. Select an IPv6 Domain Name Server (DNS) Address radio button:
   - **Get Automatically from ISP**. This is the default setting. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
   - **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. 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 router assigns IPv6 addresses to the devices on your home network (the LAN).
10. (Optional) Select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

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

    Your settings are saved.

Set up an IPv6 PPPoE Internet connection

To set up a PPPoE IPv6 Internet connection:

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

   A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Settings > Advanced Settings > IPv6**.

   The IPv6 page displays.

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

   The page adjusts.

   The 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 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 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.

6. Either select the **Use the same Login information as IPv4 PPPoE** check box (for IPv4 PPPoE information, see Specify an Internet connection that uses a login on page 30), or specify the following PPPoE login setting information for IPv6:

   a. In the **Login** field, enter the login information for the ISP connection.
   This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, you would type JerAB in this field. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.

   b. In the **Password** field, enter the password for the ISP connection.

   c. In the **Service Name** field, 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 router never terminates the connection. If the connection is terminated, for example, when the modem is turned off, the router attempts to reestablish the connection immediately after the PPPoE connection becomes available again.

7. Select an IPv6 Domain Name Server (DNS) Address radio button:
   - **Get Automatically from ISP**. This is the default setting. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
   - **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. 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 router assigns IPv6 addresses to the devices on your home network (the LAN).
9. (Optional) Select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.

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

    Your settings are saved.

Change the MTU size

The maximum transmission unit (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 NETGEAR 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 either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that does not open, or displays only part of a web page
  - Yahoo email
  - MSN portal
- You use VPN and experience severe performance problems.
- You used a program to optimize MTU for performance reasons and now you are experiencing connectivity or performance problems.

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

To change the MTU size:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > WAN Setup**.
   The WAN Setup page displays.
5. In the **MTU Size** field, enter a value from 616 to 1500.
6. Click the **Apply** button.
   Your settings are saved.

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

Table 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.)
1468	Used in some DHCP environments.
1436	Used in PPTP environments or with VPN.

4

Customize Quality of Service Settings and Optimize Gaming

You can customize Quality of Service (QoS) settings and optimize gaming by preventing network lag and congestion, by allocating bandwidth to specific devices, and by prioritizing traffic for specific devices.

This chapter contains the following sections:

Improve response time by using the Geo Filter

The main cause of lag in console games such as Call of Duty, Destiny, FIFA, and many others, is the distance from you to the host or server of the game. The Geo Filter can limit the distance of these hosts or servers by blocking all hosts or servers outside the range that you can specify. This allows for improved response time and might lead to fairer games.

Configure and use the Geo Filter

By default, no devices are added to the Geo Filter and the filter is not in effect. To start using the Geo Filter, you must add a device, specify the country or state in which your device is located, and set the distance radius for the filter.

To configure and use the Geo Filter:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Geo-Filter**.
5. To add a device to the Geo Filter, do the following in the Devices pane:
   a. Click the **ADD DEVICE** button.
      The Geo-Filter window opens and displays the detected devices.
   b. Select your device.
   c. Click **NEXT**.
   d. Select a service.
      If your device is a console, console services display. If your device is not a console, nonconsole services displays.
   e. Click **DONE**.
      The device is added to the Devices pane.
      If your device is a console, by default, the **Filtering Mode** radio button is selected for the device, which means that the router blocks connections outside your

distance radius to force your device to use a host or server inside your radius. We recommend this setting for console games.
If your device is a not console, by default, the **Spectating Mode** radio button is selected for the device, which means that the router does not block connections outside of your distance radius. We recommend this setting for most computer games which do not require filtering.

6. In the Geo-Filter Map pane, below the **Geo-Filter Map menu** icon, click the **player** icon that lets you set your home area, and move the icon to the map, more specifically, to the country or state in which your device is located.

   You can use an approximate physical location. If the map view is too small, click the **magnifying glass** icon, move it to the continent in which your gaming device is located, and click the icon again.

7. Set the distance radius by moving the **Set Distance** slider.

   We recommend that you set a distance radius in the range from 500 km to 3,000 km (311 mi. to 1,864 mi.). All connections outside the radius are prevented from hosting your game. If you set a radius that is less than 500 km (311 mi.), you might not find games. If you set a radius that is more than 3,000 km (1,864 mi.), you might not find a high-quality connection.

8. To load the recommended Geo Filter settings for your game, do the following:
   a. In the Geo-Filter pane, click the **PROFILES** button.
      The Profile Selector window opens.
   b. Select a game.
   c. Click **DONE**.

9. Play a test game.

   Play a compatible, online multiplayer game on your selected device. Blocked connections outside your radius are indicated by warning triangles and the devices whose connections are blocked are prevented from hosting your game. The host of your game is inside your radius and is indicated by the largest, most consistently shown icon.

   The following icons can be shown on the map:

   - Player
   - Blocked player (that is, a player outside the distance radius)
   - Allowed player (that is, a player that you added to the Allowlist)
   - Denied player (that is, a player that you added to the Blocklist)
   - Server

- Blocked server (that is, a server outside the distance radius)
- Allowed server (that is, a server that you added to the Allowlist)

Note: For information about allowing or blocking a connection to a device (that is, to a player or server), see Ping a device and allow or deny the device a connection on page 50.

If the Auto Ping Host option is enabled, a ping graph automatically displays when you are in a game. Otherwise, you can manually click any icon on the map to load a ping graph for that connection.

10. If a ping graph does not display for a connection, click the associated icon on the map to load the ping graph for that connection, or enable the Auto Ping Host option by doing the following:
    a. In the Geo-Filter Map pane, click the **Geo-Filter Map menu** icon.
    The Settings pane displays.
    b. Select the **Auto Ping Host** check box.
    c. Click the **X**.
    The Settings pane closes.

Ping a device and allow or deny the device a connection

You can allow or block connections to individual devices, regardless of the distance radius of your Geo Filter. If you allow an individual connection, the device can connect to your device, even if is outside the radius of your Geo Filter. If you deny an individual connection, the device cannot connect to your device, even if is inside the radius of your Geo Filter. However, you cannot block a dedicated server.

To ping a device and allow the device to connect to your device or deny the device from connecting to your device:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Geo-Filter**.

5. In the Geo-Filter Map pane, click the connection on the Geo Filter Map.

   If the Ping pane is not yet open, the Ping pane opens. For the selected connection, the Ping pane displays the ping information and the associated host type, IP address, and domain name.

   The ping results shows the connection quality from your device to the device at the other end of the connection. The connection quality is measured in milliseconds (ms). The lower the value in ms, the better.

6. In the Ping pane, do the following:
   a. To assign a name to the connection, type a name in the **Name** field.
   b. Click the **ALLOW** or **DENY** button.
      The connection is added to the Allow and Deny pane.

7. To ping the connection again, click the **ping** icon in the Allow and Deny pane.

   The new ping results display in the Ping pane.

8. To remove the connection from the Allow and Deny pane, click the **trash** icon in the Allow and Deny pane.

   If the connection was allowed, it might now be denied if it is outside the distance radius.

   If the connection was denied, it might now be allowed if it is inside the distance radius.

Add a device to the Geo Filter

You can add a device to the Geo Filter.

To add a device to the Geo Filter:

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

   A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Geo-Filter**.
5. Click the **ADD DEVICE** button.

The Geo-Filter window opens and displays the detected devices.

6. Select your device.
7. Click **NEXT**.
8. Select a service.

   If your device is a console, console services display. If your device is not a console, nonconsole services displays.

9. Click **DONE**

   The device is added to the Devices pane.

   If your device is a console, by default, the **Filtering Mode** radio button is selected for the device, which means that the router blocks connections outside your distance radius to force your device to use a host or server inside your radius. We recommend this setting for console games.

   If your device is not a console, by default, the **Spectating Mode** radio button is selected for the device, which means that the router does not block connections outside of your distance radius. We recommend this setting for most computer games which do not require filtering.

   Note: For information about using the device with the Geo Filter, see Configure and use the Geo Filter on page 48.

Remove a device from the Geo Filter

You can remove a device from the Geo Filter.

To remove a device from the Geo Filter:

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

   A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Geo-Filter**.
5. In the Devices pane, below the device that you want to remove, click the **DELETE** button.

The device is removed from the Geo Filter.

Manage the general Geo Filter map settings

You can manage the general Geo Filter map settings such as the unit of length (kilometers or miles) in which the distance radius is expressed, whether the Strict Mode feature is enabled, and whether the Auto Ping Host feature is enabled.

Fore information about using the Geo Filter, see Configure and use the Geo Filter on page 48.

To manage the general Geo Filter map settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Geo-Filter**.
5. In the Geo-Filter Map pane, click the **Geo-Filter Map menu** icon.
   The Settings pane displays.
6. Configure the following general settings:
   - **Unit of length**. By default, the **Kilometers** radio button is selected and the distance radius is shown in kilometers. You can also select the **Miles** radio button to show the distance radius in miles.
   - **Strict Mode**. The Strict Mode feature guarantees that dedicated servers that fall outside your filter range are always blocked. For most games, select the **Strict Mode** check box. For Destiny, we recommend that you keep the **Strict Mode** check box cleared. By default, the **Strict Mode** check box is selected.
   - **Auto Ping Host**. The Auto Ping Host feature automatically loads a ping graph that shows the connection quality from your device to the device at the other end of the connection. By default, the **Auto Ping Host** check box is selected. If you clear the **Auto Ping Host** check box, you can still manually ping a connection (see Ping a device and allow or deny the device a connection on page 50).

Note: The **Flush Cloud** button is for use under guidance from NETGEAR Technical Support. (Clicking the **Flush Cloud** button reloads the IP addresses for the Geo Filter.)

7. To close the Settings pane, click the **X**.

Manage bandwidth allocation

The router supports a Quality of Service (QoS) feature that lets you prevent network congestion with the Anti-Bufferbloat feature (which is a way to control the total bandwidth) and allocate bandwidth to specific devices.

Prevent network congestion with Anti-Bufferbloat

The Anti-Bufferbloat feature can prevent congestion and queuing delays that are caused by devices that consume a lot of bandwidth. You can set the maximum percentage of the total bandwidth that bandwidth-intensive devices can consume, thereby allowing bandwidth to remain available for devices that consume less bandwidth.

To configure and use the Anti-Bufferbloat feature:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **QoS**.
5. In the Anti-Bufferbloat pane, click the **Anti-Bufferbloat menu** icon.
   The Options pane displays.
6. In the **Download Bandwidth** and **Upload Bandwidth** fields, enter the total download bandwidth speed in Mbps and total upload bandwidth speed in Mbps that you receive from your ISP.
   If you are not sure about the bandwidth speeds, run a speed test, for example, by visiting speedtest.net.

7. Change the default Anti-Bufferbload options:
   - **Goodput**. By default, the **Goodput** check box is selected and both the upload and download bandwidth values are more closely aligned to the results of a speedtest. If you used the automatic Internet setup, the router performed a speed test during the setup process.
   - **Disable all QoS (not recommended)**. By default, the **Disable all QoS (not recommended)** check box is not selected. If you disable all QoS features, this will stop QoS from eliminating network congestion and it will affect other features on this router, including Deep Packet Inspection. We recommend that you do not select this check box.
8. Click the **X** to close the Options pane.
9. Select how you want to apply Anti-Bufferbloat:
   - **Always**. Select this radio button if you want to always apply Anti-Bufferbloat. If Anti-Bufferbloat is always applied, you can play games without any devices or applications causing you to lag but your total bandwidth speeds is reduced so you must change the setting back to **Never** when you finish gaming.
   - **When High Priority Traffic Detected**. Select this radio button if you only want to apply Anti-Bufferbloat when games are being played (all console games and most computer games are automatically detected by DumaOS). Your total bandwidth speeds will only be reduced when games are detected. This radio button is selected by default.
   - **Never**. Select this radio button to disable Anti-Bufferbloat. If Anti-Bufferbload is disabled, your full bandwidth speeds are received but your games are caught in a queue, causing lag, when all your bandwidth is being used.
10. In the Anti-Bufferbloat pane, move the buttons on the **Download** and **Upload** sliders to the desired percentage values.

    To the right of each slider, the selected value displays are a percentage of the total bandwidth speed that you specified in Step 6 and as an absolute value in Mb.

    For example, if you move the button on the **Download** slider to 70, devices that consume a lot of bandwidth are limited to 70 percent of the total bandwidth speed that you specified, and 30 percent of the total bandwidth remains available for devices that consume less bandwidth.

Disable Anti-Bufferbloat

If you disable the Anti-Bufferbloat feature, bandwidth-intensive devices can consume all available bandwidth, causing congestion and forcing traffic for other devices to be

queued. However, situations might exist in which you want to disable the Anti-Bufferbloat feature.

To disable the Anti-Bufferbloat feature:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **QoS**.
5. In the Anti-Bufferbloat pane, move the buttons on the **Download** and **Upload** sliders all the way to the right, to 100 percent.
   The Anti-Bufferbloat feature is now disabled.

Allocate bandwidth to devices

Some devices on your network need more bandwidth than others. For example, a device that you use for gaming or media streaming requires more bandwidth than a device that is mostly used for browsing and emails. You can allocate a percentage of the total router bandwidth to each of the devices on your network. Doing so guarantees bandwidth for a device when it needs it.

You can set different allocations for upload and download bandwidths.

By default, the router automatically allocates excess (unused) bandwidth to a device that needs it. Although we do not recommend it, you can disable this option so that the router does not share unused bandwidth across your network and the bandwidth that you allocate to each device is the maximum bandwidth that the device can use.

To allocate bandwidth to devices:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **QoS**.
   The Bandwidth Allocation pane displays a graph that shows the devices on the router network. By default, each device is allocated an equal share of the router bandwidth, expressed by a number in a white circle that is associated with a device.

5. To allocate download bandwidth to devices, do the following in the Bandwidth Allocation pane:
   a. Above the graph, select the **Download** radio button.
      By default, this radio button is selected. The Bandwidth Allocation pane shows as the Bandwidth Allocation - Download pane.
   b. For each device to which you want to allocate download bandwidth, move the associated white circle to the bandwidth percentage that you want to allocate. As you move the white circle, the download percentages in the white circles for other devices change.

      CAUTION: If you allocate 100 percent to one device, you effectively disable other devices. If you allocate 0 percent to one device, you effectively disable the device.

   c. Click the **UDATE DISTRIBUTION** button.
      The allocated download bandwidths take effect.

6. To allocate upload bandwidth to devices, do the following in the Bandwidth Allocation pane:
   a. Above the graph, select the **Upload** radio button.
      The Bandwidth Allocation pane shows as the Bandwidth Allocation - Upload pane.
   b. For each device to which you want to allocate upload bandwidth, move the associated white circle to the bandwidth percentage that you want to allocate. As you move the white circle, the download percentages in the white circles for other devices change.

      CAUTION: If you allocate 100 percent to one device, you effectively disable other devices. If you allocate 0 percent to one device, you effectively disable the device.

   c. Click the **UDATE DISTRIBUTION** button.
      The allocated upload bandwidths take effect.

7. To allocate an exact bandwidth (either in Mbps or in percentage) to a device, do the following in the Bandwidth Allocation pane:
   a. Above the graph, select either the **Download** radio button or **Upload** radio button.
   b. From the list of devices to the left of the graph, select the device.
      If no devices display, click the **+** to the left of Devices.
      A pane opens on the right side.
   c. Do *one* of the following:
      - In the **Set Device Bandwidth** field, enter the bandwidth in Mbps.
      - In the **Set Device Bandwidth** field, use the up or down arrows to set the bandwidth.
      - In the circle graph, move the red band to the desired bandwidth percentage.
      - In the field that shows the percentage, enter the desired bandwidth percentage.
   d. Click the **SAVE** button.
      The allocated bandwidth takes effect.
      Bandwidth that you allocate to this device also affects available bandwidth for other devices.
   e. To close the pane, click the **X**.

8. To prevent unused bandwidth from being shared across your network (which we do not recommend), do the following in the Bandwidth Allocation pane:
   a. Click the **Bandwidth Allocation menu** icon.
      The Settings pane opens.
   b. Clear the **Share Excess** check box.
      The bandwidth that you allocate to each device is now the maximum bandwidth that the device can use. This setting applies to both the download bandwidth and upload bandwidth.
   c. To close the Settings pane, click the **X**.

Reset the bandwidth distribution

You can reset the bandwidth to default settings so that the router allocates each device an equal share of the bandwidth. You can reset the bandwidth distribution for download bandwidth and upload bandwidth separately.

To reset the bandwidth to default settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **QoS**.
   The Bandwidth Allocation pane displays a graph that shows the devices on the router network. By default, each device is allocated an equal share of the router bandwidth, expressed by a number in a white circle that is associated with a device.
5. Above the graph, select either the **Download** radio button or **Upload** radio button.
   If you reset the download bandwidth, the allocated upload bandwidths are not affected. The other way around is also true: If you reset the upload bandwidth, the allocated download bandwidths are not affected.
6. Click the **RESET DISTRIBUTION** button.
   The default bandwidths take effect.

Manage traffic prioritization

The router supports a Quality of Service (QoS) feature that lets you prioritize traffic for specific devices.

Prioritize traffic for a device and view prioritization information

By default, the router automatically prioritizes high-priority traffic such as games. If you prefer, you can manually disable automatic traffic prioritization (see Disable automatic traffic prioritization on page 62).

Whether or not automatic traffic prioritization is enabled, you can prioritize the traffic for a device and service so that, if network congestion occurs, the traffic is not held up in a queue but is sent to the front of the queue, reducing network lag for the device. Traffic prioritization for a device affects both outgoing and incoming traffic.

You can also view traffic prioritization information. The router shows the number of uploaded and downloaded packets that were sent to the front of the queue and shows whether high-priority traffic is automatically prioritized.

To prioritize traffic for a device and view prioritization information:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **QoS**.
5. Scroll down to the Traffic Prioritization pane.
   By default, traffic prioritization for DumaOS classified games is enabled. DumaOS classified games is a preset list of games and covers all console games and most PC games. If you enable traffic prioritization for all DumaOS classified games, your router automatically applies traffic prioritization when it detects games. We recommend that you keep this setting enabled.
   You can manually add your own service or port/port range by clicking the **ADD DEVICE** button and then choosing the service or port/port range you would like to add.
6. To manually add a device for traffic prioritization, do the following in the Devices pane:
   a. From the All Devices section, clear the **Enabled** check box.
      Your router no longer automatically applies traffic prioritization when it detects games.
   b. Click the **ADD DEVICE** button.
      The Traffic Prioritization Selector window opens and the detected devices display.
   c. Select your device.
   d. Select a service.
      By default, the **Basic** radio button is selected and a preset list of games display. We recommend that you manually select a service only if you consider yourself an advanced user.

e. To display other selection criteria, select the **Advanced** radio button, and enter the start and end numbers for the source port, enter the start and end numbers for the destination port, and select the protocol.

f. Click **DONE**.
The device is added to the Traffic Prioritization pane and its traffic is now prioritized.
The Traffic Prioritization Information pane displays the total number of high-priority packets, the total number of background packets, and the total number of unprioritized packets. This information is displayed for both uploaded packets and downloaded packets.
If high-priority traffic is automatically being prioritized, a colored circle displays in the Traffic Prioritization Information pane next to High Priority Traffic Detected.

Add a device for traffic prioritization

You can add a device for traffic prioritization.

To add a device for traffic prioritization:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **QoS**.
5. Scroll down to the Traffic Prioritization pane.
6. From the All Devices section, clear the **Enabled** check box.
   Your router no longer automatically applies traffic prioritization when it detects games.
7. Click the **ADD DEVICE** button.
   The Traffic Prioritization Selector window opens and the detected devices display.
8. Select your device.
9. Select a service.

By default, the **Basic** radio button is selected and a preset list of games display. We recommend that you manually select a service only if you consider yourself an advanced user.

10. To display other selection criteria, select the **Advanced** radio button, and enter the start and end numbers for the source port, enter the start and end numbers for the destination port, and select the protocol.
11. Click **DONE**.

    The device is added to the Traffic Prioritization pane.

Stop traffic prioritization for a device

You can stop traffic prioritization for a device that you manually added to the Traffic Prioritization pane. If automatic traffic prioritization is enabled (which it is by default) and the router detects high-priority traffic to or from the device, the router still prioritizes that traffic. However, other traffic to or from the device is no longer prioritized.

To stop traffic prioritization for a device:

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **QoS**.
5. Scroll down to the Traffic Prioritization pane and click the **trash** icon next to the device.

   The device is removed from the Traffic Prioritization pane.

Disable automatic traffic prioritization

By default, the router automatically prioritizes high-priority traffic such as games. You can disable this option.

To disable the automatic traffic prioritization:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **QoS**.
5. Scroll down to the Traffic Prioritization pane.
6. From the All Devices section, clear the **Enabled** check box.
   High-priority traffic is no longer automatically prioritized.

5

Monitor Devices and the Network and View Router Information

This chapter describes how to monitor the devices on your network and the network itself and how to view the router system information.

For more information about viewing the router logs, statistics, and network connection, see Maintain the Router on page 119.

The chapter includes the following sections:

View and manage devices currently on the network

You can view all computers and devices that are currently connected to your router network. You can change the settings that display on the page (you cannot change the actual settings for a device through the router), prevent a device from being displayed, and block a device from connecting to the Internet through router.

To view and manage devices on the network:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Device Manager**.
   The Network Map page displays, showing the device tree with your network setup. The device tree shows separate branches for devices connected through the wired LAN and devices connected over WiFi, as well as a branch for the WAN connection.
5. To display the settings for a device, click the device.
   The Device Settings pane displays. The pane shows the MAC address, IP address (if any), and connection type for the device.
6. To assign or change the displayed name and type for the device, in the Device Settings pane, do the following:
   a. In the **Name** field, enter a name of up to 35 characters.
   b. From the **Device Type** menu, select a type.
   c. Click the **SAVE** button.
      Your settings are saved.
7. To remove the device from the network tree, in the Device Settings pane, click the **DELETE** button.
   The device no longer displays in the device tree. This option is useful when a device is removed from the network and you no longer want to see it in the device tree.

8. To block a device from accessing the Internet through the router, in the Device Settings pane, click the **BLOCK** button.

   The device is blocked and is indicated by a black icon in the device tree.

9. To unblock a previously blocked device so that it can once again access the Internet through the router, in the Device Settings pane, click the **UNBLOCK** button.

   The device is unblocked and is indicated by a red icon in the device tree.

View network usage information

The router integrates deep packet inspection (DPI) so that you can view the devices, traffic categories, and applications that are using the upload and download bandwidth in your router network. You can then use this information to apply your Quality of Service (QoS) settings and optimize gaming (see Customize Quality of Service Settings and Optimize Gaming on page 47).

You can view real-time information about all devices on your network that are consuming bandwidth and you can view details about traffic categories and applications that are consuming bandwidth for a device. You also view the total bandwidth usage across the router network relative to the network's overall bandwidth speeds.

To view network usage information:

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

   A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Network Monitor**.

   The page that displays shows the Network Snapshot pane and the Network Overview pane:

   - **Network Snapshot pane**. This pane displays the upload and download network bandwidth in Mbps per second. The pane displays the total usage as well as individual usage for active devices.
   - **Network Overview pane**. This pane displays the network's total bandwidth usage in Mbps per second, relative to the network's overall bandwidth speeds.

5. To view upload or download volume details, point to a bar (in the Network Snapshot pane) or point to a node (in the Network Overview pane).

   A small pop-up window displays volume details.

6. To limit the displayed bandwidth in a pane to the download bandwidth or upload bandwidth, do the following:

   - To exclude upload bandwidth from the pane, above the graph in a pane, click the **Upload** text.
     The Upload text is crossed out and the graph displays the download bandwidth only. Click the **Upload** text again to redisplay the upload bandwidth.
   - To exclude download bandwidth from the pane, above the graph in a pane, click the **Download** text.
     The Download text is crossed out and the graph displays the upload bandwidth only. Click the **Download** text again to redisplay the download bandwidth.

7. To view the traffic category breakdown for the total usage or for an individual device, in the Network Snapshot pane, click the download or upload bar for either the total usage or for an individual device.

   The Category Breakdown pane displays and shows the traffic categories that are using download or upload bandwidth for your selection.

   You can take any of the following actions in the Category Breakdown pane:

   - To view traffic category volume details, point to the graph.
     A small pop-up window displays volume details.
   - To exclude a traffic category from the graph, above the graph, click the name for the traffic category.
     The name is crossed out and the graph excludes the traffic category. Click the name for the category again to redisplay the traffic category.
   - To view the applications that are consuming bandwidth for your selection and traffic category, click the graph.
     The Application Breakdown pane displays and shows the applications that are using download or upload bandwidth for your selection.
     You can take any of the following actions in the Application Breakdown pane:
     - To view application volume details, point to the graph.
       A small pop-up window displays volume details.
     - To exclude an application from the graph, above the graph, click the name for the application.
       The name is crossed out and the graph excludes the application. Click the name for the application again to redisplay the application.
     - To close the Application Breakdown pane, click the **X**.

- To close the Category Breakdown pane, click the **X**.

View router system information

To view router system information:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **System Information**.
   The page that displays shows the following panes:
   - **CPU Usage**. This pane shows usage information about both CPUs on the router. You can take any of the following actions in the CPU Usage pane:
     - To exclude a CPU from the graph, above the graph, click the name of the CPU.
       The name is crossed out and the graph excludes information about the CPU. Click the name of the CPU again to redisplay information about the CPU.
     - To view usage details about a CPU, point to a node on the graph.
       A small pop-up window displays usage details.
   - **RAM Usage**. This pane shows usage information about the three random access memory (RAM) categories on the router. You can take any of the following actions in the RAM Usage pane:
     - To exclude a RAM category from the graph, above the graph, click the name of the RAM category.
       The name is crossed out and the graph excludes information about the RAM category. Click the name of the RAM category again to redisplay information about the RAM category.
     - To view usage detail about a RAM category, point to the graph.
       A small pop-up window displays usage details.

- **Flash Usage**. This pane shows usage information about the eight flash memory categories on the router. You can take any of the following actions in the Flash Usage pane:
  - To exclude a flash memory category from the graph, above the graph, click the name of the flash memory category.
    The name is crossed out and the graph excludes information about the flash memory category. Click the name of the flash memory category again to redisplay information about the flash memory category.
  - To view usage details about a flash memory, point to the graph.
    A small pop-up window displays usage details.
- **System Info**. The information in this pane includes the firmware version that is installed on the router.
- **Network Status**. This pane shows the bytes and packets that the router transferred since it was started, including deprioritized packets.
- **Installed R-Apps**. This pane shows the default router applications (R-Apps) that are installed on the router. Do not change the retry-attempts-on-startup value in the Options pane that is accessible from the Installed R-Apps pane, unless Technical Support instructs you to do so.
- **Internet Status**. The information in this pane includes the WAN IP address of the router.
- **Wireless Status**. The information in this pane includes the network key (WiFi password) for the main WiFi network.
- **Guest Wireless Status**. This information in this pane includes the network key (WiFi password) for the guest WiFi network.
- **Logs**. This pane shows the logs. You can also download the logs as a text file.

Customize the dashboard

By default, the Dashboard includes the following panes:

- Internet Status
- Wireless Status
- Guest Wireless Status
- Network Overview
- CPU Usage
- Installed R-Apps

For information about these panes, see View router system information on page 68.

You can customize the panes that display on the Dashboard by adding panes that are useful to you and removing panes that are not useful to you. You also rearrange and resize the panes.

To customize the Dashboard:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. To add panes to the Dashboard, do the following:
   a. Select **Geo-Filter**, **QoS**, **Device Manager**, **Network Monitor**, or **System Information**.
      The page displays panes.
   b. For each pane that you want to add, click the **pin** icon that is associated with the pane.
      The panes are added to the Dashboard.
5. To remove a pane from the Dashboard, on the Dashboard, click the **pin** icon that is associated with the pane.
   The pane is removed from the Dashboard but not from its home page.
6. To move a pane to another location on the Dashboard, do the following:
   a. Point to a pane until the cursor displays as a cross with four arrows.
   b. Click and hold the pane and move it to another location.
   c. Release the pane.
7. To resize a pane, do the following:
   a. Point to a pane until the diagonal double-headed arrow displays at the lower right corner of the pane.
   b. Click the arrow and move the pane horizontally, vertically, or both.
   c. Release the pane.

6

Control Access to the Internet

The router comes with a built-in firewall that helps protect your home network from unwanted intrusions from the Internet.

This chapter includes the following sections:

Block access to Internet sites

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.

Add keywords and block access to specific Internet sites

You can add keywords to block specific Internet sites from your network. You can use blocking all the time or based on a schedule.

To add keywords and block access to select Internet sites:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Content Filtering > Block Sites**.
   The Block Sites page displays.
5. Select a keyword blocking option:
   - **Per Schedule**. Turn on keyword blocking according to a schedule that you set. For more information, see Set up a schedule for keyword blocking and outbound firewall rules on page 77.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule page.
6. In the **Type keyword or domain name here** field, enter a keyword or domain that you want to block.
   Website names and domain names that include the keyword are blocked or the domain name that you specify is blocked.
   For example:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.

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

7. Click the **Add Keyword** button.
   The keyword is added to the keyword list. The keyword list supports up to 255 entries.
8. Click the **Apply** button.
   Keyword blocking takes effect.

Delete keywords from the blocked list

To delete one or all keywords from the list:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Content Filtering > Block Sites**.
   The Block Sites page displays.
5. Do one of the following:
   - To delete a single word, select it and click the **Delete Keyword** button.
     The keyword is removed from the list.
   - To delete all keywords on the list, click the **Clear List** button.
     All keywords are removed from the list.
6. Click the **Apply** button.
   Your settings are saved.

Avoid blocking on a trusted computer

You can exempt one trusted computer from blocking. The computer that you exempt must be assigned a fixed IP address. You can use the reserved IP address feature to specify the IP address (see Manage reserved LAN IP addresses on page 88).

To specify a trusted computer:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Content Filtering > Block Sites**.
   The Block Sites page displays.
5. Scroll down and select the **Allow trusted IP address to visit blocked sites** check box.
6. In the **Trusted IP Address** field, enter the IP address of the trusted computer.
7. Click the **Apply** button.
   Your settings are saved.

Block services and applications with simple outbound firewall rules

A firewall protects one network (the trusted network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two.

The router provides one default outbound firewall rule: It allows all access to the Internet (that is, the WAN). You can add simple rules to prevent access to specific services and applications on the Internet. In addition, you can specify if a rule applies to one user, a range of users, or all users on your LAN.

The router lists many default services and applications that you can use in outbound rules. You can also add an outbound firewall rule for a custom service or application.

For information about blocking specific keywords, URLs, or sites, see Block access to Internet sites on page 72. This type of blocking is another aspect of outbound firewall rules.

Note: Service blocking means the same thing as applying outbound firewall rules.

Block a service or application from accessing the Internet

You can block Internet services on your network based on the type of service. You can block the services all the time or based on a schedule.

To block a service or application from accessing the Internet:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings> Content Filtering > Block Services**.
   The Block Services page displays.
5. Specify when to block the services:
   - To block the services all the time, select the **Always** radio button.
   - To block the services based on a schedule, select the **Per Schedule** radio button.

   For information about how to specify the schedule, see Set up a schedule for keyword blocking and outbound firewall rules on page 77.
6. Click the **Add** button.
   The Block Services Setup page displays.
7. To add a service that is in the **Service Type** menu, select the application or service.
   The settings for this service automatically display in the fields.
8. To add a service or application that is not in the menu, select **User Defined**, and do the following:
   a. If you know that the application uses either TCP or UDP, select the appropriate protocol from the **Protocol** menu. Otherwise, select **TCP/UDP** (both).
   b. Enter the starting port and ending port numbers.
      If the service uses a single port number, enter that number in both fields. To find out which port numbers the service or application uses, you can contact the publisher of the application, ask user groups or newsgroups, or search on the Internet.
   c. In the **Service Type/User Defined** field, enter a description.

9. Select a filtering option:
   - **Only This IP Address**. Block services for a single computer. Enter the IP address for that computer.
   - **IP Address Range**. Block services for a range of computers with consecutive IP addresses on your network. Enter the starting IP address and ending IP address for the range.
   - **All IP Addresses**. Block services for all computers on your network.
10. Click the **Add** button.
    Your settings are saved.

Change an outbound firewall rule for a service or application

You can change an existing outbound firewall rule that blocks a service or application.

To change an outbound firewall rule for a service or application:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Content Filtering > Block Services**.
   The Block Services page displays.
5. In the Service Table, select the radio button for the rule.
6. Click the **Edit** button.
   The Block Services Setup page displays.
7. Change the settings.
   For more information about the settings, see Block a service or application from accessing the Internet on page 75.
8. Click the **Accept** button.

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

Remove an outbound firewall rule for a service or application

You can remove an outbound firewall rule that you no longer need. After you remove the rule, the service or application is no longer blocked.

To remove an outbound firewall rule for a service or application:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Content Filtering > Block Services**.
   The Block Services page displays.
5. In the Service Table, select the radio button for the rule.
6. Click the **Delete** button.
   The rule is removed from the Service Table.

Set up a schedule for keyword blocking and outbound firewall rules

You can set up a schedule that you can apply to keyword blocking for Internet sites and outbound firewall rules for services and applications.

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 blocking (see Block access to Internet sites on page 72), outbound firewall rules (see Block services and applications with simple outbound firewall rules on page 74), or both. Without a schedule, you can only enable or disable these features. By default, no schedule is set.

To set up a schedule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Content Filtering > Schedule**.
   The Schedule page displays.
5. Set up the schedule for blocking:
   - **Days to Block**. Select the check box for each day that you want to block access or specify that blocking occurs on every day by selecting the **Every Day** check box.
     By default, the **Every Day** check box is selected.
   - **Time of Day to Block**. Select a start and end time for blocking in 24-hour format or select the **All Day** check box for 24-hour blocking.
     By default, the **All Day** check box is selected.
6. From the **Time Zone** menu, select your time zone.
7. If you live in an area that observes daylight saving time, select the **Automatically adjust for daylight savings time** check box.

   Note: If the router synchronized its internal clock with a time server on the Internet and you selected the correct time zone, the **Current Time** field displays the correct date and time.

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

Set up email notifications for security events and log messages

The router can email you notifications of security events and its log messages of router activity. The log records router activity and security events such as attempts to access blocked sites, services, or applications.

To set up email notifications:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Content Filtering > E-mail**.
   The E-mail page displays.
5. Select the **Turn E-mail Notification On** check box.
6. In the **Primary E-mail Address** field, enter the email address that you want to send alerts and logs to.
7. In the **Your Outgoing Mail Server** field, enter the name of your ISP outgoing (SMTP) mail server (such as mail.myISP.com).
   You might be able to find this information in the configuration window of your email program. If you leave this field blank, log and alert messages are not sent.
8. In the **Outgoing Mail Server Port Number** section, enter the port number that your outgoing mail server uses.
   The default port number is 25. If your ISP uses a different port number, you might be able to find this information in the configuration window of your email program.
9. If your outgoing email server requires authentication, select the **My mail server requires authentication** check box, and do the following:
   a. In the **User Name** field, type the user name for the outgoing email server.
   b. In the **Password** field, type the password for the outgoing email server.

10. To send 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. This is the default setting.

11. To send logs messages based on a schedule, select a schedule from the **Send logs according to this schedule** menu and specify the settings:

    - **Hourly**. The router sends log messages hourly.
    - **Daily**. The router sends log messages daily at the time that you specify. From the **Time** menu, select the time, and select the **a.m.** or **p.m.** radio button.
    - **Weekly**. The router sends log messages weekly at the day and time that you specify. From the **Day** menu, select the day of the week. From the **Time** menu, select the time, and select the **a.m.** or **p.m.** radio button.

    By default, the router sends log messages when the log is full. To prevent the router from doing so, select **None** from the **Send logs according to this schedule** menu.

12. Click the **Apply** button.

    Your settings are saved.

    The router sends log messages automatically according to the schedule that you set. If the log fills before the specified time, the router sends all log messages. After the router sends the log messages, they are cleared from the router memory. If the router cannot send the log messages and the log buffer fills, the router overwrites the log messages.

7

Manage the Router's Network Settings

The router comes ready for WiFi, Ethernet, and USB connections. You can customize the router's network settings. We recommend that you install the router and connect it to the Internet before you change its network settings.

This chapter includes the following sections:

View or change WAN settings

You can view or configure wide area network (WAN) settings for the Internet port. You can set up a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the router to respond to a ping to its WAN (Internet) port.

To view or change the WAN settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > WAN Setup**.
   The WAN Setup page displays.
   View or change the following settings:
   - **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, and many others. Select this check box only in special circumstances.
   - **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing, but it makes the firewall security less effective. For more information, see Set up a default DMZ server on page 83.
   - **Respond to Ping on Internet Port**. This feature allows your router to be discovered. Use this feature only as a diagnostic tool or for a specific reason.
   - **Disable IGMP Proxying**. IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. By default, the **Disable IGMP Proxying** check box is selected and IGMP proxying is disabled.
   - **MTU Size (in bytes)**. The normal maximum transmit unit (MTU) value for most Ethernet networks is 1500 bytes (which is the default setting), or 1492 bytes for PPPoE connections. Change the MTU value only if you are sure that it is necessary for your ISP connection. For more information, see Change the MTU size on page 44.
   - **NAT Filtering**. Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT protects computers on the LAN from

attacks from the Internet but might prevent some Internet games, 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. By default, the **Secured NAT** radio button is selected and the router functions with secured NAT.

- **Disable SIP ALG**. Some voice and video communication applications do not work well with the SIP ALG. Disabling the SIP ALG might help your voice and video applications to create and accept a call through the router.

5. If you made changes to the settings, click the **Apply** button.
   Your settings are saved.

Set up a default DMZ server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The 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 router usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or a service that you configured on the Port Forwarding/Port Triggering page. Instead of discarding this traffic, you can specify that the router forwards the traffic to one computer on your network. This computer is called the default DMZ server.

To set up a default DMZ server:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **Settings > Setup > WAN Setup**.
   The WAN Setup page displays.
5. Select the **Default DMZ Server** check box.
6. Type the IP address.
7. Click the **Apply** button.
   Your settings are saved.

Change the router's device name

The router's default device name is based on its model number. This device name displays in, for example, the file manager when you browse your network. If you change this name, the ReadySHARE storage folder access path automatically changes to reflect the new device name.

To change the router's device name:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Setup > Device Name**.
   The Device Name page displays.
5. In the **Device Name** field, type a new name.
6. Click the **Apply** button.
   Your settings are saved.

Change the router's LAN IP address and RIP settings

The router is preconfigured to use private IP addresses on the LAN side and to function as a DHCP server. The router's default LAN IP configuration is as follows:

- **LAN IP address**. 192.168.1.1
- **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. If your network requires a different IP addressing scheme, you can change these settings.

You might want to change these settings if you need a specific IP subnet that one or more devices on the network use, or if you use competing subnets with the same IP scheme.

To change the LAN IP address and RIP settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > LAN Setup**.
   The LAN Setup page displays.
5. In the **IP Address** field, type the IP address.
6. In the **IP Subnet Mask** field, type the subnet mask of the router.
   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.

7. Router Information Protocol (RIP) allows a router to exchange routing information with other routers. To change the RIP settings, do the following:
   a. Select the RIP direction:
      - **Both**. The router broadcasts its routing table periodically and incorporates information that it receives. This is the default setting.
      - **Out Only**. The router broadcasts its routing table periodically.
      - **In Only**. The router incorporates the RIP information that it receives.

   b. Select the RIP version:
      - **Disabled**. The RIP versions are ignored. 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-2**. This format carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

8. Click the **Apply** button.
   Your settings are saved.
   If you changed the LAN IP address of the router, you are disconnected when this change takes effect.
9. To reconnect, close your browser, relaunch it, and log in to the router.

Specify the IP addresses that the router assigns

By default, the router functions as a Dynamic Host Configuration Protocol (DHCP) server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the router.

These addresses must be part of the same IP address subnet as the router's LAN IP address. If you changed the router's LAN IP address (see Change the router's LAN IP address and RIP settings on page 85), the addresses must be part of the IP address subnet of the router's new LAN IP address.

If you use the router's default addressing scheme, define a range between 192.168.1.2 and 192.168.1.254, although you can save part of the range for devices with fixed addresses.

To specify the pool of IP addresses that the router assigns:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > LAN Setup**.
   The LAN Setup page displays.
5. Make sure that the **Use Router as DHCP Server** check box is selected.
6. Specify the range of IP addresses that the router assigns:
   a. In the **Starting IP Address** field, type the lowest number in the range.
      This IP address must be in the same subnet as the router.
   b. In the **Ending IP Address** field, type the number at the end of the range of IP addresses.
      This IP address must be in the same subnet as the router.
7. Click the **Apply** button.
   Your settings are saved.
   The 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 (the router's LAN IP address)
   - DNS server IP address (the router's LAN IP address)

Disable the DHCP server in the router

By default, the router functions as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the router.

You can use another device on your network as the DHCP server or specify the network settings of all your computers.

To disable the DHCP server in the router:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > LAN Setup**.
   The LAN Setup page displays.
5. Clear the **Use Router as DHCP Server** check box.
6. Click the **Apply** button.
   Your settings are saved.
7. (Optional) If this service is disabled and no other DHCP server is available on your network, set your computer IP addresses manually so that the computers can access the router.

Manage reserved LAN IP addresses

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the router's DHCP server. Assign reserved IP addresses to computers or servers that require permanent IP settings.

Reserve a LAN IP address

To reserve a LAN IP address:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.

The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **Settings > Setup > LAN Setup**.
   The LAN Setup page displays.
5. In the Address Reservation section, click the **Add** button.
   The Address Reservation page displays.
6. Either add a device that the router detected and that is in the Address Reservation Table or add a custom device:
   - To add a device that the router detected and that is in the Address Reservation Table, select the radio button for the device.
     The **IP Address** field, **MAC Address** field, and **Device Name** field are populated with the information from the the Address Reservation Table.
   - To add a custom device, do the following:
     a. In the **IP Address** field, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.1.x.
     b. In the **MAC Address** field, type the MAC address of the computer or server.
     c. In the **Device Name** field, type a description for the computer or server.
7. Click the **Add** button.
   The LAN Setup page displays again and the address is entered into the Address Reservation table on that page.
8. Click the **Apply** button.
   Your settings are saved.

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

Change a reserved IP address

To change a reserved address entry:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.

3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > LAN Setup**.
   The LAN Setup page displays.
5. Select the radio button next to the reserved address.
6. Click the **Edit** button.
   The Address Reservation page displays.
7. Change the settings.
8. Click the **Apply** button.
   The LAN Setup page displays again. The Address Reservation table on that page shows the changed settings.
9. Click the **Apply** button.
   Your settings are saved.

Delete a reserved IP address entry

To delete a reserved address entry:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > LAN Setup**.
   The LAN Setup page displays.
5. Select the radio button next to the reserved address.
6. Click the **Delete** button.
   The address is removed from the Address Reservation table.

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

Set up a bridge to your ISP's network using a port group or VLAN tag group

Some devices, such as an IPTV, cannot function behind the 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 the bridge between the device and the router's Internet port or add new VLAN tag groups to the bridge.

Note: If your ISP provides instructions for how to set up a bridge for IPTV and Internet service, follow those instructions.

Set up a bridge to your ISP's network using a port group

For some devices, such as an IPTV, that are connected to the router's Ethernet LAN port or WiFi network, your ISP might require you to use a port group to set up a bridge to the router's Internet interface and, effectively, your ISP's network.

A bridge with a port group prevents packets that are sent between the device and the router's Internet port from being processed through the router's Network Address Translation (NAT) service.

For an IPTV-specific procedure, see Set up an IPTV port to lease an intranet port on page 94.

To set up a bridge to your ISP's network using a port group:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > VLAN/Bridge Settings**.
   The VLAN/Bridge Settings page displays.

5. Select the **Enable VLAN/Bridge group** check box.
   The page expands.
6. Select the **By bridge group** radio button.
   The page expands.
7. Select a Wired Ports check box or a Wireless check box:
   - If your device is connected to an Ethernet port on the router, select the Wired Ports check box that corresponds to the Ethernet port on the router to which the device is connected.
   - If your device is connected to your router's WiFi network, select the Wireless check box that corresponds to the router's WiFi network to which the device is connected.

   Note: You must select at least one Wired Ports or Wireless check box. You can select more than one check box.
8. Click the **Apply** button.
   Your settings are saved.

Set up a bridge to your ISP's network using a VLAN tag group

For some devices, such as IPTVs, that are connected to the router's Ethernet LAN ports or WiFi network, your ISP might require you to use a VLAN tag group to set up a bridge to the router's Internet interface and, effectively, your ISP's network.

If you are subscribed to a service such as IPTV, the router might require VLAN tags to distinguish between the Internet traffic and the IPTV traffic. A bridge with a VLAN tag group prevents packets that are sent between the device and the router's Internet port from being processed through the router's Network Address Translation (NAT) service.

You can add VLAN tag groups to a bridge and assign VLAN IDs and priority values to each VLAN tag group.

To set up a bridge to your ISP's network using a VLAN tag group:

1. Launch a web browser from a computer or mobile device that is connected to the network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **Settings > Advanced Settings > VLAN/Bridge Settings**.
   The VLAN/Bridge Settings page displays.
5. Select the **Enable VLAN/Bridge group** check box.
   The page expands.
6. Select the **By VLAN tag group** radio button.
   The page expands.
7. Click the **Add** button.
   The Add VLAN Rule page displays.
8. Specify the following settings:
   - **Name**. Enter a name for the VLAN tag group. The name can be up to 10 characters.
   - **VLAN ID**. Enter a value from 1 to 4094.
   - **Priority**. Enter a value from 0 to 7.
   - Select the check box for a wired LAN port or WiFi port.
     - If your device is connected to an Ethernet port on the router, select the LAN port check box that corresponds to the Ethernet port on the router to which the device is connected.
     - If your device is connected to your router's WiFi network, select the WiFi check box that corresponds to the router's WiFi network to which the device is connected.

     You must select at least one LAN port or WiFi port. You can select more than one port.
9. Click the **Add** button.
   The VLAN/Bridge Settings page displays again. The VLAN tag group is added to the table on that page.
10. Click the **Apply** button.
    Your settings are saved.

Set up an IPTV port to lease an intranet port

You can set up the router to create an Internet Protocol television (IPTV) port that can lease an IP address from your IPTV service provider. Use this feature only if you subscribe to an IPTV service and your IPTV service requires an intranet address.

Some IPTV ports cannot work behind NAT because the IPTV port requires an IP address within the Internet service provider's network (intranet address). You can set up a bridge connection from the WAN to one of the LAN ports. When IPTV is connected through WiFi, the home router also must support the bridging of the WAN port to the WiFi network name (SSID). The designated LAN port or WiFi network name becomes an IPTV port with direct access to the WAN without going through NAT.

To set up an IPTV port to lease an intranet port from your IPTV service provider:

1. Launch a web browser from a computer or mobile device that is connected to the network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > VLAN/Bridge Settings**.
   The VLAN / Bridge Settings page displays.
5. Select the **Enable VLAN/Bridge Group** check box.
   The page expands.
6. Select the **By bridge group** radio button.
   The page expands.
7. Depending on the port to which the IPTV is connected, select a Wired Ports check box or a Wireless check box:
   - If the IPTV is connected to an Ethernet port on the router, select the Wired Ports check box that corresponds to the Ethernet port on the router to which the device is connected.
   - If the IPTV is connected to your router's WiFi network, select the Wireless check box that corresponds to the router's WiFi network to which the device is connected.
8. Click the **Apply** button.
   Your settings are saved.

Manage custom static routes

Typically, you do not need to add static routes unless 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 main Internet access is through a cable modem to an ISP.
- Your home network includes an ISDN router for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.
- Your company's network address is 134.177.0.0.

When you set up your 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 192.168.1.x addresses. With this configuration, if you try to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the company firewall is likely to deny the request.

In this case you must define a static route, telling your router to access 134.177.0.0 through the ISDN router at 192.168.1.100. Here is an example:

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** field specifies that all traffic for these addresses will be forwarded to the ISDN router at 192.168.1.100.
- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

Set up a static route

To set up a static route:

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **Settings > Advanced Settings > Static Routes**.
   The Static Routes page displays.
5. Click the **Add** button.
   The page adjusts.
6. In the **Route Name** field, type a name for this static route (for identification purposes only).
7. To limit access to the LAN only, select the **Private** check box.
   If the **Private** check box is selected, the static route is not reported in RIP.
8. Select the **Active** check box to make this route effective.
9. In the **Destination IP Address** field, type the IP address of the final destination.
10. In the **IP Subnet Mask** field, type the IP subnet mask for this destination.
    If the destination is a single host, type **255.255.255.255**.
11. In the **Gateway IP Address** field, type the gateway IP address, which must be on the same LAN segment as the router.
12. In the **Metric** field, type a number from 2 through 15 as the metric value.
    This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.
13. Click the **Apply** button.
    The static route is added to the table.

Change a static route

To change a static route:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > Static Routes**.

The Static Routes page displays.

5. In the table, select the radio button for the route.
6. Click the **Edit** button.
   The Static Routes page adjusts.
7. Edit the route information.
8. Click the **Apply** button.
   Your settings are saved.

Delete a static route

To delete a static route:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > Static Routes**.
   The Static Routes page displays.
5. In the table, select the radio button for the route.
6. Click the **Delete** button.
   The route is removed from the table.

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.

To manage Universal Plug and Play:

1. Launch a web browser from a computer or mobile device that is connected to the network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The default password is **password**. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Setting > UPnP**.
   The UPnP page displays.
5. If UPnP is not enabled, select the **Turn UPnP On** check box.
   By default, this check box is selected. You can disable UPnP for automatic device configuration. If you clear the **Turn UPnP On** check box, the router does not allow any device to automatically control router resources, such as port forwarding.
6. Type the advertisement period in minutes.
   The advertisement period specifies how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points receive current device status at the expense of more network traffic. Longer durations can compromise the freshness of the device status but can significantly reduce network traffic.
7. Type the advertisement time to live in hops.
   The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. Hops are the steps a packet takes between routers. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.
8. Click the **Apply** button.
   The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the 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.

9. To refresh the information in the UPnP Portmap Table, click the **Refresh** button.

8

Manage the Router’s WiFi Settings

The router comes ready for WiFi connections. You can customize the router’s WiFi settings.

This chapter includes the following sections:

Specify basic WiFi settings

The router comes with preset security. This means that the WiFi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the router label.

Note: The preset SSID and password are uniquely generated for every device to protect and maximize your WiFi security.

If you change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

If your computer is connected with WiFi when you change the SSID or other WiFi security settings, you are disconnected when you click the **Apply** button. To avoid this problem, use a computer with a wired connection to access the router.

You can specify the settings for the 2.4 GHz band and for the 5 GHz band. However, if you enable Smart Connect, the 2.4 GHz and 5 GHz bands must use the same WiFi network name (SSID) and network key (password).

To specify basic WiFi settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > Wireless Setup**.
   The Wireless Settings page displays.
   You can specify the settings for the 2.4 GHz band and 5 GHz band.
5. From the **Region** menu, select your region.
   In some locations, you cannot change this setting.
6. To let the router automatically select the fastest WiFi band (2.4 GHz or 5 GHz) for your device, select the **Enable Smart Connect** check box.
   By default, the **Enable Smart Connect** check box is selected and both the **Name (SSID)** field and radio buttons for the security options for the 5 GHz band are masked out because that band uses the same network name (SSID) and security option as

the 2.4 GHz band. That means that when you connect to the router with WiFi, you see only one SSID that connects to both bands.

Note: If you enable Smart Connect and the SSID and passwords for the 2.4 GHz and 5 GHz bands do not match, the SSID and security option for the 2.4 GHz band overwrite the SSID and security option for the 5 GHz band.

To specify a separate SSID and security option for each WiFi band, clear the **Enable Smart Connect** check box.

7. To control the SSID broadcast, select or clear the **Enable SSID Broadcast** check box.

   When this check box is selected, the router broadcasts its SSID so that it displays when you scan for local WiFi networks on your computer or mobile device.

8. To control 20/40 MHz coexistence, select or clear the **Enable 20/40 MHz Coexistence** check box.

   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.

9. To change the network name (SSID), type a new name in the **Name (SSID)** field.

   The name can be up to 32 characters long and it is case-sensitive. The default SSID is randomly generated and is on the router label . If you change the name, make sure to write down the new name and keep it in a safe place.

10. To change the WiFi channel, select a number from the **Channel** menu.

    In some regions, not all channels are available. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

    When you use multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is four channels (for example, use Channels 1 and 5, or 6 and 10).

    Note: For information about the options in the **Mode** menu, see Change the WiFi mode for download and upload speeds on page 104. By default, the fastest modes are selected.

11. Click the **Apply** button.

    Your settings are saved.

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

12. Make sure that you can connect wirelessly to the network with its new settings.

    If you cannot connect wirelessly, check the following:

    - Is your computer or mobile device connected to another WiFi network in your area? Some mobile devices automatically connect to the first open network without WiFi security that they discover.
    - Is your computer or mobile device trying to connect to your network with its old settings (before you changed the settings)? If so, update the WiFi network selection in your computer or mobile device to match the current settings for your network.

Change the WiFi password or security level

The WiFi password is different from the admin password that you use to log in to the router.

Your router comes with preset WPA2 or WPA security. We recommend that you use the preset security, but you can change the settings. We recommend that you do not disable the preset security.

For information about other WiFi security options, see Configure WPA/WPA2 enterprise WiFi security on page 106 and Configure WEP legacy WiFi security on page 108.

To change the WPA settings:

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Setup > Wireless Setup**.

   The Wireless Settings page displays.
5. Under Security Options, select a WPA option.

   The WPA2 options use the newest standard for the strongest security. WPA2-PSK [AES] is the default setting.

The **Passphrase** field displays.

6. In the **Passphrase** field, enter the network key (password).
   It is a text string from 8 to 63 characters.
7. Write down the new password and keep it in a secure place for future reference.
8. Click the **Apply** button.
   Your settings are saved.
9. 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:
   - Is your computer or mobile device connected to another WiFi network in your area? Some mobile devices automatically connect to the first open network without WiFi security that they discover.
   - Is your computer or mobile device trying to connect to your network with its old settings (before you changed the settings)? If so, update the WiFi network selection in your computer or mobile device to match the current settings for your network.

Change the WiFi mode for download and upload speeds

The data rate for high-speed transmissions is commonly identified as megabits per second (Mbps).

By default, the router is set to operate with up to 800 Mbps in the 2.4 GHz WiFi band and up to 1,733 Mbps in the 5 GHz WiFi band. You can select slower settings.

To change the WiFi mode settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > Wireless Setup**.

The Wireless Settings page displays.

5. For the 2.4 GHz WiFi band, in the Wireless Network (2.4 GHz b/g/n) section, select a setting from the **Mode** menu.

   Up to 800 Mbps is the default setting. The other settings are Up to 347 Mbps and Up to 54 Mbps.

6. For the 5 GHz WiFi band, select a setting from the **Mode** menu.

   Up to 1733 Mbps is the default setting, which allows 802.11ac, 11n, and 11ad devices to join the network. The other settings are Up to 800 Mbps and Up to 347 Mbps.

7. Click the **Apply** button.

   Your settings are saved.

   If you are connected over WiFi to the network, you might be disconnected from the network and might need to reconnect.

Set up a guest WiFi network

Guest networks allow visitors at your home to use the Internet without using your WiFi security key. You can add a guest network for the 2.4 GHz WiFi band and the 5.0 GHz WiFi band.

By default, the guest networks are disabled.

To set up a guest network:

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

   A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Settings > Setup > Guest Network**.

   The Guest Network Settings page displays.

5. Scroll to the section of the page for the guest WiFi network that you want to set up.
6. Leave the **Enable SSID Broadcast** check box selected.

Allowing the router to broadcast its WiFi network name (SSID) makes it easier to find your network and connect to it. If you clear this check box, that creates a hidden network.

7. If you want to allow mobile devices that are connected to the guest network to detect each other and provide access to your main WiFi network, select the **Allow guests to see each other and access my local network** check box.

   For greater security, by default, mobile devices that are connected to the guest WiFi network cannot detect each other or access mobile devices or Ethernet devices that are connected to the main WiFi network.

8. Keep the default guest network name or type a custom name.

   The default guest WiFi network names (SSIDs) are as follows:

   - **NETGEAR-Guest** is for the 2.4 GHz WiFi band.
   - **NETGEAR-5G-Guest** is for the 5 GHz WiFi band.

   The guest network name is case-sensitive and can be up to 32 characters. You can configure the WiFi-enabled devices in your network to use the guest network name in addition to the main SSID.

9. Select a security option.

   The WPA2 options use the newest standard for the strongest security. WPA2-PSK [AES] is the default setting.

   For information about WPA/WPA2 Enterprise, see Configure WPA/WPA2 enterprise WiFi security on page 106.

10. To enable the guest network, select the **Enable Guest Network** check box.

    If you do not select this check box, the guest network settings are saved after you click the **Apply** button, but the guest network remains disabled.

11. Click the **Apply** button.

    Your settings are saved.

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

Tip: If you want to change the WiFi settings of the router's main network, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

To configure WPA and WPA2 enterprise security:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Depending on the WiFi network that you are configuring, do one of the following:
   - If you are configuring the main WiFi network, select **Settings > Setup > Wireless Setup**.
     The Wireless Settings page displays.
   - If you are configuring the guest WiFi network, select **Settings > Setup > Guest Network**.
     The Guest Network page displays.
5. In the Security Options section for either the 2.4 GHz band or 5 GHz band, select the **WPA/WPA2 Enterprise** radio button.
   The page adjusts.
6. In the WPA/WPA2 Enterprise section, specify the following settings:
   - From the **WPA Mode** menu, select the enterprise WPA mode:
     - **WPA2 [AES]**. WPA2 provides a secure connection but some older mobile devices do not detect WPA2 and support only WPA. If your network includes such older devices, select WPA [TKIP] + WPA2 [AES] security.
     - **WPA [TKIP] +WPA2 [AES]**. This type of security enables mobile devices that support either WPA or WPA2 to join the router's WiFi network. This is the default mode.
   - **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 router that is used to access the RADIUS server for authentication. The default port number is 1812.

- **RADIUS server Shared Secret**. Enter the shared secret (RADIUS password) that is used between the router and the RADIUS server during authentication of a WiFi user.

7. Click the **Apply** button.
   Your settings are saved.
8. 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:
   - Is your computer or mobile device connected to another WiFi network in your area? Some mobile devices automatically connect to the first open network without WiFi security that they discover.
   - Is your computer or mobile device trying to connect to your network with its old settings (before you changed the settings)? If so, update the WiFi network selection in your computer or mobile device to match the current settings for your network.

Configure WEP legacy WiFi security

Wired Equivalent Privacy (WEP) security is a legacy authentication and data encryption mode that is superseded by WPA-PSK and WPA2-PSK. WEP limits the WiFi transmission speed to 54 Mbps (the router is capable of speeds of up 800 Mbps in the 2.4 GHz band).

Tip: If you want to change the WiFi settings of the router's main network, use a wired connection to avoid being disconnected when the new WiFi settings take effect.

To configure WEP security:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.

4. Depending on the WiFi network that you are configuring, do one of the following:

   - If you are configuring the main WiFi network, do the following:
     a. Select **Settings > Setup > Wireless Setup**.
        The Wireless Settings page displays.
     b. From the **Mode** menu, select **Up to 54 Mbps**.
        The page adjusts to display the **WEP** radio button.

   - If you are configuring the guest WiFi network, select **Settings > Setup > Guest Network**.
     The Guest Network page displays.

     Note: You can configure WEP security for the guest network only if the selection from the **Mode** menu for the *main* WiFi network is **Up to 54 Mbps**. You cannot set the WiFi mode for the guest network separately from the main WiFi network.

5. In the Security Options section, select the **WEP** radio button.
   The page adjusts.

6. From the **Authentication Type** menu, select one of the following types:

   - **Automatic**. Clients can use either Open System or Shared Key authentication.
   - **Shared Key**. Clients can use only Shared Key authentication.

7. From the **Encryption Strength** menu, select the encryption key size:

   - **64-bit**. Standard WEP encryption, using 40/64-bit encryption.
   - **128-bit**. Standard WEP encryption, using 104/128-bit encryption. This selection provides higher encryption security.

8. Specify the active key by selecting the **Key 1**, **Key 2**, **Key 3**, or **Key 4** radio button.
   Only one key can be the active key. To join the router's WiFi network, a user must enter the key value for the key that you specified as the active key.

9. Enter a value for the key:

   - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, A–F). The key values are not case-sensitive.
   - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, A–F). The key values are not case-sensitive.

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

11. 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:

    - Is your computer or mobile device connected to another WiFi network in your area? Some mobile devices automatically connect to the first open network without WiFi security that they discover.
    - Is your computer or mobile device trying to connect to your network with its old settings (before you changed the settings)? If so, update the WiFi network selection in your computer or mobile device to match the current settings for your network.

Control the WiFi radios

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

You can turn the WiFi radios on and off with the **WiFi On/Off** button on the router, or you can log in to the router and enable or disable the WiFi radios. If you are close to the router, it might be easier to press its **WiFi On/Off** button. If you are away from the router or already logged in it might be easier to enable or disable them.

Use the WiFi On/Off button

To turn the WiFi radios off and on with the WiFi On/Off button:

Press the **WiFi On/Off** button on the top of the router for two seconds.

If you turned off the WiFi radios, the WiFi On/Off LED and the WPS LED turn off. If you turned on the WiFi radios, the WiFi On/Off LED and the WPS LED light.

Enable or disable the WiFi radios using the router web interface

If you used the **WiFi On/Off** button to turn off the WiFi radios, you can't use a WiFi connection to log in to the router to turn them back on. You must press the **WiFi On/Off** button again for two seconds to turn the WiFi radios back on.

To enable or disable the WiFi radios:

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

   A login window opens.

3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Advanced Wireless**.
   The Advanced Wireless Settings page displays.
5. In the 2.4 GHz and 5 GHz sections, select or clear the **Enable Wireless Router Radio** check boxes.
   Clearing these check boxes turns off the WiFi feature of the router for each band.
6. Click the **Apply** button.

   Note: If you turned off both WiFi radios, the WiFi On/Off LED and the WPS LED turn off. If you turned on the WiFi radios, the WiFi On/Off LED and the WPS LED light.

Use the WPS Wizard for WiFi connections

The WPS Wizard helps you connect WPS-enabled devices to your WiFi network without typing the WiFi password.

You can use the WPS Wizard or you can use the physical **WPS** button on your router to connect WPS-enabled devices. To use the physical **WPS** button on your router, see WiFi connection using WPS on page 21 for more information.

To use the WPS Wizard to connect to the WiFi network:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Setup > WPS Wizard**.
   The Add WPS Client page displays.
5. Click the **Next** button.

The page displays instructions about how to connect using WPS.

6. Click the **WPS** button that displays on the page.

   Note: To use the physical **WPS** push button on the router, see WiFi connection using WPS on page 21 and follow the instructions in that section.

7. Within two minutes, go to the WPS-enabled device and use its WPS software to connect to the WiFi network.

   A success page displays if your WPS-enabled device successfully connects to the WiFi network.

Set up a WiFi schedule

You can turn off the WiFi signal from your router at times when you do not need a WiFi connection. For example, you might turn it off for the weekend if you leave town.

To set up the WiFi schedule:

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

   A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

4. Select **Settings > Advanced Settings > Advanced Wireless**.

   The Advanced Wireless Settings page displays.

5. Click the **Add a new period** button.

   The page adjusts.

6. Use the menus, radio buttons, and check boxes to set up a period during which you want to turn off the WiFi signal.
7. Click the **Apply** button.

   The Advanced Wireless Settings page displays.

8. To activate the schedule, select the **Turn off wireless signal by schedule** check box.

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

Specify WPS settings

Wi-Fi Protected Setup (WPS) lets you join the WiFi network without typing the WiFi password.

To specify WPS settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Advanced Wireless**.
   The Advanced Wireless Settings page displays.
   The Router's PIN field displays the fixed PIN that you can use to configure the router's WiFi settings from another device through WPS.
5. (Optional) Select or clear the **Enable Router's PIN** check box.
   The PIN function might temporarily be disabled when the router detects suspicious attempts to break into the router's WiFi settings by using the router's PIN through WPS. (By default, after three such attempts, the PIN function is temporarily disabled.) You can manually enable the PIN function by selecting the **Enable Router's PIN** check box.
6. (Optional) Select or clear the **Keep Existing Wireless Settings** check box.
   By default, the **Keep Existing Wireless Settings** check box is selected. We recommend that you leave this check box selected.
   If you clear this check box, the next time a new WiFi client uses WPS to connect to the router, the router WiFi settings change to an automatically generated random SSID and security key.
7. Click the **Apply** button.
   Your settings are saved.

Manage implicit beamforming

Beamforming shapes a directional WiFi signal aimed at a WiFi client based on the client's location, as opposed to radiating the signal out in all directions. This feature improves WiFi range and performance. Clients do not need to support beamforming to benefit from implicit beamforming.

To disable implicit beamforming:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Advanced Wireless**.
   The Advanced Wireless Settings page displays.
5. Scroll to the bottom of the page and clear the **Enable Implicit BEAMFORMING** check box.
6. Click the **Apply** button.
   Your settings are saved.
   If you are connected over WiFi to the network, you might be disconnected from the network and might need to reconnect.

Manage MU-MIMO

Multi user 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. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Advanced Wireless**.
   The Advanced Wireless Settings page displays.
5. Scroll to the bottom of the page and clear the **Enable MU-MIMO** check box.
6. Click the **Apply** button.
   Your settings are saved.
   If you are connected over WiFi to the network, you might be disconnected from the network and might need to reconnect.

Manage HT160 for 160 MHz WiFi support

HT160 supports 160 MHz for WiFi traffic, reducing lag and improving gaming and streaming data speeds. Note that the WiFi clients that connect to the router must be capable of supporting 160 MHz, and they must be connected to the 5 GHz WiFi network. By default, HT160 is disabled, but you can enable it.

To enable HT160:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Advanced Wireless**.

The Advanced Wireless Settings page displays.

5. Scroll to the bottom of the page and select the **Enable HT160** check box.
6. Click the **Apply** button.
   Your settings are saved.

   If you are connected over WiFi to the network, you might be disconnected from the network and might need to reconnect.

Disable Wi-Fi Multimedia Quality of Service

Wi-Fi Multimedia Quality of Service (WMM QoS) prioritizes WiFi voice and video traffic over the 2.4 GHz band. By default, WMM QoS is enabled for the router.

WMM QoS prioritizes WiFi data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, WMM must be enabled for both it and the client running that application. Legacy applications that do not support WMM and applications that do not require QoS are assigned to the best effort category, which receives a lower priority than voice and video.

Note: We recommend that you do not disable the WMM settings. If you disable the WMM settings, the maximum link rate your router can reach is 54 Mbps over the 2.4 GHz band.

To disable the WMM settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > Advanced Wireless**.
   The Advanced Wireless Settings page displays.
5. Clear the **Enable WMM (Wi-Fi multimedia) settings (2.4GHz b/g/n)** check box.
6. Click the **Apply** button.

Your settings are saved.

Use the router as a WiFi access point only

By default, the router functions both as a router and a WiFi access point (AP). You can set up the router to function in AP mode and let it operate on the same local network as another router. When the router functions in AP mode, many of its router-related features are disabled.

To use the router in AP mode:

1. Use an Ethernet cable to connect the Internet port of this router to an Ethernet port on the other router.
2. Launch a web browser from a computer or mobile device that is connected to the network.
3. Enter **http://www.routerlogin.net**.
   A login window opens.
4. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
5. Select **Settings > Setup > Router Mode**.
   The Router / AP Mode page displays. By default the **Router Mode** radio button is selected and the router functions both as a router and a WiFi AP.
6. Select the **AP Mode** radio button.
   The page adjusts.
7. Select an IP address setting:
   - **Get dynamically from existing router**. The other router on the network assigns an IP address to this router while this router is in AP mode.
   - **Use fixed IP Address (not recommended)**. Use this setting if you want to manually assign a specific IP address to this router that the router uses while it functions in AP mode. Using this option effectively requires advanced network experience.

   Note: To avoid interference with other routers or gateways in your network, we recommend that you use different WiFi settings on each router. You can also turn off the WiFi radio on the other router, access point, or gateway and use this router only for WiFi client access.

8. Click the **Apply** button.
   The IP address of the router changes, and you are disconnected.
9. To reconnect, close and restart your browser and type **http://www.routerlogin.net**.

9

Maintain the Router

This chapter describes the settings for administering and maintaining your router.

For information about monitoring devices and the network and viewing the router system information, see Monitor Devices and the Network and View Router Information on page 64.

The chapter includes the following sections:

Update the router firmware

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

Check for new firmware and update the router

The router firmware (routing software) is stored in flash memory. You might see a message at the top of the router pages when new firmware is available. You can respond to that message to update the firmware or you can check to see if new firmware is available and update the router.

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

To check for new firmware and update your router:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Administration > Firmware Update**.
   The Firmware Update page displays.
5. Click the **Check** button.
   The router finds new firmware information if any is available and displays a message asking if you want to download and install it.
6. Click the **Yes** button.
   The router locates and downloads the firmware and begins the update.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the router.

The router restarts after the firmware is uploaded and updated. The update process typically takes about one minute. Read the new firmware release notes to find out if you must reconfigure the router after updating.

7. To verify that the router installed the new firmware, do the following:
   a. If the login window does not open automatically, enter **http://www.routerlogin.net** in your web browser.
   b. Enter the router admin user name and password.
      The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
      The Dashboard displays.
   c. Select **System Information**.
      The page that displays shows multiple panes.
      The firmware version is listed in the System Info pane.

8. To enable the router to automatically update to future firmware versions as they become available, do the following:
   a. Select **Settings > Administration > Firmware Update**.
      The Firmware Update page displays.
   b. In the Router Auto Firmware Update section, select the **I Agree** radio button.
   c. Click the **Apply** button.
      Your settings are saved.

Manually upload firmware to the router

If you want to upload a specific firmware version, or your router fails to update its firmware automatically, follow these instructions.

Note: We recommend that you connect a computer to the router using an Ethernet connection to upload the firmware.

To manually upload a firmware file to your router:

1. Download the firmware for your router from the NETGEAR Download Center, save it to your desktop, and unzip the file if needed.

   Note: The correct firmware file uses an `.img` extension.

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

3. Launch a web browser from a computer or mobile device that is connected to the router network.
4. Enter **http://www.routerlogin.net**.
   A login window opens.
5. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
6. Select **Settings > Administration > Firmware Update**.
   The Firmware Update page displays.
7. Click the **Browse** button.
8. Find and select the saved firmware file on your computer.
9. Click the **Upload** button.
   The router begins the update.

   WARNING: To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the router.

   The router restarts after the firmware is uploaded and updated. The update process typically takes about one minute.
10. To verify that the router installed the new firmware, do the following:
    a. If the login window does not open automatically, enter **http://www.routerlogin.net** in your web browser.
    b. Enter the router admin user name and password.
       The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
       The Dashboard displays.
    c. Select **System Information**.
       The page that displays shows multiple panes.
       The firmware version is listed in the System Info pane.

Change the admin password

The first time that you logged in to the router with the user name admin, you were required to change the password. You can change this password again. This password is not the one that you use for WiFi access.

Note: Be sure to change the password to a secure password. 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 admin password:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Administration > Set Password**.
   The Set Password page displays.
5. Type the old password in the **Old Password** field.
   This is the password that you specified the first time that you logged in to the router.
6. Type the new password in the **Set Password** and **Repeat New Password** fields.
7. Click the **Apply** button.
   Your settings are saved.

Enable admin password reset

The router admin password is used to log in to your router web interface. We recommend that you enable password reset so that you can reset the password if you forget it. This reset process is supported in Chrome, Safari, Firefox, Edge, and Internet Explorer.

To enable password reset:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **Settings > Administration > Set Password**.
   The Set Password page displays.
5. Select the **Enable Password Reset** check box.
6. Select two security questions and provide answers to them.
7. Click the **Apply** button.
   Your settings are saved.

Reset the admin password

If you set up the password reset feature, you can reset your router admin password if you forgot it. This reset process is supported in Chrome, Safari, Firefox, Edge, and Internet Explorer.

To reset your router admin password:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Click the **Cancel** button.
   If password reset is enabled, you are prompted to enter the serial number of the router.
   The serial number is on the router label.
4. Enter the serial number of the router.
5. Click the **Continue** button.
   The Router Password Reset page displays.

6. Enter the answers to your security questions.
7. Click the **Continue** button.
   The page adjusts.
8. Type a new admin password, confirm your new password, and set new security questions and answers.
9. Click the **Next** button.
   The page displays a confirmation.
10. Click the **Login** button.
    A login window opens.
11. With your new password, log in to the router.

Manage the router configuration file

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

Back up the configuration settings

To back up the router's configuration settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Administration > Backup Settings**.
   The Backup Settings page displays.
5. Click the **Back Up** button.
6. Follow the direction of your browser to save the file.
   A copy of the current settings is saved in the location that you specified.

Restore the configuration settings

To restore the configuration settings that you backed up:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Administration > Backup Settings**.
   The Backup Settings page displays.
5. Click the **Browse** button to find and select the `.cfg` file.
6. Click the **Restore** button.
   The file is uploaded to the router and the router restarts.

   WARNING: Do not interrupt the restoration process.

Erase the current configuration settings

You can erase the current configuration and restore the factory default settings. You might want to do this if you move the router to a different network.

To erase the configuration settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Administration > Backup Settings**.

The Backup Settings page displays.

5. Click the **Erase** button.
   The factory default settings are restored and the router restarts.

   WARNING: Do not interrupt the restart process.

   After the restart process is complete, the user name is admin, the password is password, and the LAN IP address is 192.168.1.1. DHCP is enabled.

Manage remote access

You can access your router over the Internet to view or change its settings. You must know the router's WAN IP address to use this feature.

Note: If you did not specify a secure password the first time that you logged in to the router with the user name admin, be sure to change the password to a secure password. 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 (see Change the admin password on page 123).

Set up remote management

To set up remote management:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > Remote Management**.
   The Remote Management page displays.
5. Select the **Turn Remote Management On** check box.
6. 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:

- **Only This Computer**. Allow access from a single IP address on the Internet. Enter the IP address to be allowed access.
- **IP Address Range**. Allow access from a range of IP addresses on the Internet. Enter a beginning IP address and an ending IP address to define the allowed range.
- **Everyone**. Allow access from any IP address on the Internet.

7. Specify the port number for accessing the router web interface.
   Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote router web interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default is 8443, which is a common alternate for HTTP.
8. Click the **Apply** button.
   Your settings are saved.

Use remote access

To use remote access:

1. Launch a web browser on a computer that is not on your home network.
2. Type your router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number.
   For example, if your external address is 134.177.0.123 and you use port number 8443, enter **http://134.177.0.123:8443** in your browser.

Access your router using the Nighthawk app

You can use the Nighthawk app to access your router and change its settings. Before you can use access with the Nighthawk app, you must update your router's firmware and download the latest Nighthawk app for your mobile device.

For more information about how to update your router's firmware, see Update the router firmware on page 120.

To download the latest Nighthawk app for your mobile device, visit https://www.netgear.com/home/apps-services/nighthawk-app/.

Monitor and meter Internet traffic

Traffic metering allows you to monitor the volume of Internet traffic that passes through the router Internet port. With the traffic meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

Start the traffic meter without traffic volume restrictions

You can monitor the traffic volume without setting a limit.

To start or restart the traffic meter without configuring traffic volume restrictions:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Monitoring > Traffic Meter**.
   The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
   By default, no traffic limit is specified and the traffic volume is not controlled.
6. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
7. To start the traffic counter immediately, click the **Restart Counter Now** button.
8. Click the **Apply** button.
   Your settings are saved and the router restarts.
   The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics on page 132.

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 by volume.

To record and restrict the Internet traffic by volume:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Monitoring > Traffic Meter**.
   The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
6. Select the **Traffic volume control by** radio button.
7. From the corresponding menu, select an option:
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
8. In the **Monthly Limit** field, enter how many MBytes (MB) per month are allowed.
9. If your ISP charges you for extra data volume when you make a new connection, enter the extra data volume in MB in the **Round up data volume for each connection by** field.
10. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
11. In the **Pop up a warning message** field, enter a value in minutes to specify when the router issues a warning message before the monthly limit in hours is reached.
    This setting is optional. The 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.
12. Select one or more of the following actions to occur when the limit is reached:
    - **Turn the Internet LED to flashing white/amber**. This setting is optional. When the traffic limit is reached, the Internet LED blinks alternating white and amber.
    - **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.
13. Click the **Apply** button.
    Your settings are saved and the router restarts.

The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics on page 132.

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. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Monitoring > Traffic Meter**.
   The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
6. Select the **Connection time control** radio button.

   Note: The router must be connected to the Internet for you to be able to select the **Connection time control** radio button.

7. In the **Monthly Limit** field, enter how many hours per month are allowed.

   Note: The router must be connected to the Internet for you to be able to enter information in the **Monthly Limit** field.

8. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
9. In the **Pop up a warning message** field, enter a value in minutes to specify when the router issues a warning message before the monthly limit in hours is reached.
   This setting is optional. The 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.

10. Select one or more of the following actions to occur when the limit is reached:
    - **Turn the Internet LED to flashing white/amber**. This setting is optional. When the traffic limit is reached, the Internet LED alternates blinking white and amber.
    - **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.
11. Click the **Apply** button.

    Your settings are saved and the router restarts.

    The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics on page 132.

View the Internet traffic volume and statistics

If you enabled the traffic meter (see Start the traffic meter without traffic volume restrictions on page 129), you can view the Internet traffic volume and statistics.

To view the Internet traffic volume and statistics shown by the traffic meter:

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Monitoring > Traffic Meter**.

   The Traffic Meter page displays.
5. Scroll down to the Internet Traffic Statistics section.

   The Internet Traffic Statistics section displays when the traffic counter was started and what the traffic balance is. The table displays information about the connection time and traffic volume in MB.
6. To refresh the information on the page, click the **Refresh** button.

   The information on the page is updated.
7. To display more information about the data traffic and to change the polling interval, click the **Traffic Status** button.

   The Traffic Status pop-up window displays.

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. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Monitoring > Traffic Meter**.
   The Traffic Meter page displays.
5. In the Traffic Control section, clear the **Disconnect and disable the Internet connection** check box.
6. Click the **Apply** button.
   Your settings are saved and the router restarts.

View and manage the router activity log

The log is a detailed record of many router actions, including the websites that you and others accessed or attempted to access. The router can store up to 256 entries in the log.

If you set up content filtering (see Control Access to the Internet on page 71), the log shows you when someone on your network tried to access a blocked site, service, or application. If you set up email notification (see Set up email notifications for security events and log messages on page 79), the router can send you the log entries in an email message.

To view and manage the log:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Monitoring > Logs**.
   The Logs page displays. Depending on the type of log entry, a log entry can show any of the following information:
   - **Action**. The action that occurred, such as whether Internet access was blocked or allowed.
   - **Source IP**. The IP address of the initiating device for this log entry.
   - **Target address**. The name or IP address of a website or news group visited or to which access was attempted.
   - **Date and time**. The date and time the log entry was recorded.
5. To customize the log, scroll down and clear or select the check boxes for the type of events that you want to be included.
   By default, the check boxes for all types of events are selected.
6. To refresh the log page, click the **Refresh** button.
   The information on the page is updated.
7. To email the log entries immediately, click the **Send Log** button.
   The log entries are emailed to the email address that you specified for the router (see Set up email notifications for security events and log messages on page 79).
8. If you changed the settings in Step 5, click the **Apply** button.
   Your settings are saved.

   Note: Before you clear the log entries, we recommend that you email the log entries (see Step 7) or download them to your computer (see Step 10).
9. To clear the log entries, click the **Clear Log** button.
   All log entries are removed.

10. To download the log entries as a text file to your computer, do the following:
    a. Select **System Information**.
       The page that displays shows multiple panes.
    b. Scroll down to the Logs pane and click the **Logs menu** icon.
       The Filters pane displays.
    c. Click the **DOWNLOAD LOG FILE** button.
       The log entries are downloaded to your computer as a text file.
    d. To close the Filter pane, click the **X**.

Display Internet port statistics

To display Internet port statistics:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Monitoring > Statistics**.
   The page that display shows a table with the following statistics information:
   - **System Up Time**. The time elapsed since the router was last restarted.
   - **Port**. The statistics for the WAN (Internet) port, LAN (Ethernet) ports, and WLANs (WiFi networks). For each port, the page 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.

5. To change the polling frequency, enter a time in seconds in the **Poll Interval** field and click the **Set Interval** button.
6. To stop the polling entirely, click the **Stop** button.

Check the Internet connection status, view details, and release and renew the connection

To check the Internet connection status if the router is connected to a WAN Ethernet connection and view details about the connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Click **Settings > Monitoring > Connection Status**.
   The Connection Status page displays. The information that shows on the page depends on the type of WAN Ethernet interface connection for the router. For the most common type of connection, in which the router receives an IP address dynamically from the ISP, the page shows the following information:
   - **IP Address**. The IP address that is assigned to the router.

     Note: If the IP address is shown as 0.0.0.0, the router did not obtain an IP address for its WAN Ethernet interface.

   - **Subnet Mask**. The subnet mask that is assigned to the router.

- **Default Gateway**. The IP address for the default gateway that the router communicates with.
- **DHCP Server**. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.
- **DNS Server**. The IP address of the Domain Name Service server that provides translation of network names to IP addresses.
- **Lease Obtained**. The date and time when the IP address lease was obtained from the ISP's DHCP server.
- **Lease Expires**. The date and time that the IP address lease expires.

5. To release the IP address lease, which causes all fields to be reset to 0, click the **Release** button.
6. To renew the IP address lease, click the **Renew** button.

   In most situations, the ISP's DHCP server assigns the same IP address to the router, but it is possible that the ISP's DHCP server assigns a different IP address to the router.

Restart the router from its web interface

You can restart the router remotely from its web interface.

To restart the router:

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **System Information**.

   The page that displays shows multiple panes.
5. In the System Info pane, click the **System Info menu** icon.

   The Options pane displays.

6. Click the **REBOOT** button.
   A pop-up window displays a warning.
7. In the pop-up window, click the **REBOOT** button.
   The router restarts.

View router notifications

The router might generate notifications.

To view router notifications:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. In the upper left, click the **bell** icon.
   The Notifications pane displays.
5. To close the pane, click the **X**.

Disable or enable LED blinking or turn off LEDs

Log in to the router to disable or enable LED blinking. You can also turn off the LEDs.

Note: To turn off all LEDs except the Power LED, you can also use the LED **On/Off** switch on the rear panel of the router (see Turn the LEDs on or off using the LED On/Off switch on page 18).

To disable LED blinking or turn off the LEDs using the router web interface:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > LED Control Settings**.
   The LED Control Settings page displays.
5. Select an LED control setting:
   - **Enable blinking on Internet LED, LAN LED, Wireless LED and USB LED when data traffic is detected**. Allows standard LED behavior. This setting is enabled by default.
   - **Disable blinking on Internet LED, LAN LED, Wireless LED and USB LED when data traffic is detected**. Blinking is disabled when data traffic is detected.
   - **Turn off all LEDs except Power LED**. All the LEDs, except the Power LED, are turned off.
6. Click the **Apply** button.
   Your settings are saved.

10

Share USB Storage Devices Attached to the Router

This chapter describes how to access and manage storage devices attached to your router. ReadySHARE® lets you access and share USB storage devices connected to the router. (If your storage device uses special drivers, it is not compatible.)

Note: The USB ports on the router can be used only to connect USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, CD drives, or DVD drives to the router USB port.

This chapter contains the following sections:

For more information about ReadySHARE features, visit netgear.com/readyshare.

USB device requirements

The router works with most USB-compliant external flash and hard drives. For the most up-to-date list of USB devices that the 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 router.

The 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 router

ReadySHARE lets you access and share USB storage devices that are connected to a USB port on the router. (If your USB storage device uses special drivers, it is not compatible.)

To connect a USB device:

1. Insert your USB storage device into a USB port on the 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 router.

   When you connect the USB storage device to the router 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 on your local area network (LAN).

Access a storage device connected to the router from a Windows-based computer

To access the USB storage device from a Windows-based computer:

1. Connect a USB storage device to a USB port on your 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 router.

   When you connect the USB storage device to the 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 on your local area network (LAN).
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.

Map a USB device to a Windows network drive

To map the USB storage device to a Windows network drive:

1. Connect a USB storage device to a USB port on your 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 router.

   When you connect the USB storage device to the 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 on your local area network (LAN).
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.
   b. Click the **OK** button.

Access a storage device that is connected to the router from a Mac

From a computer or device on the network, you can access a storage device that is connected to the router.

To access the device from a Mac:

1. Connect a USB storage device to a USB port on your 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 router.

   When you connect the USB storage device to the 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 on your local area network (LAN).
3. On a Mac that is connected to the network, select **Go > Connect to Server**.
   The Connect to Server window displays.
4. In the **Server Address** field, enter **smb://readyshare**.
5. When prompted, select the **Guest** radio button.
6. Click the **Connect** button.
   A window automatically opens and displays the files and folders on the USB storage device.

Back up Windows-based computers with ReadySHARE Vault

Your router comes with free backup software for all the Windows-based computers in your home. Connect a USB hard disk drive (HDD) to the 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 your Windows-based computer:

1. Connect a USB HDD storage device to a USB port on the 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 router.

   When you connect the USB storage device to the 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 on your local area network (LAN).
3. Download ReadySHARE Vault from netgear.com/readyshare and install it on each Windows-based computer.
4. Launch ReadySHARE Vault.
5. Use the dashboard or the **Backup** tab to set up and run your backup.

Back up Mac computers with Time Machine

You can use Time Machine to back up your Mac computers onto a USB hard drive that is connected to a USP port on the router. You can access the connected storage device from your Mac with a wired or WiFi connection to your router.

Note: The following instructions might be different depending on the macOS your computer is using. For more instructions about backing up your computer with Time Machine, see the Apple support site.

Set up a USB hard drive on a Mac

We recommend that you use a new USB HDD or format your old USB HDD to do the Time Machine backup for the first time. Use a blank partition to prevent some issues during backup using Time Machine. The router supports GUID or MBR partitions.

To format your USB hard disk drive and specify partitions:

1. Physically connect the USB HDD to your 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 router.

   When you connect the USB HDD to the 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 on your local area network (LAN).
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 computer.
2. Verify and repair the backup disk and the local disk.
3. Verify and 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 grayed 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

You can use Time Machine to back up your Mac computers onto a USB hard disk drive (HDD) that is connected to a USB port on the router.

To back up your Mac onto a USB hard disk drive:

1. Prepare your USB device with a compatible format and partitions.
   For more information, see Set up a USB hard drive on a Mac on page 145.
2. If you plan to back up a large amount of data, see Prepare to back up a large amount of data on page 145.
3. If your USB HDD uses a power supply, connect it.
   You must use the power supply when you connect the USB HDD to the router.

   When you connect the USB HDD to the 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 on your local area network (LAN).
4. On a Mac computer that is connected to the network, launch Finder and select **Go > Connect to Server**.
   The Connect to Server window opens.

5. Type **smb://routerlogin.net** and click the **Connect** button.
6. When prompted, select the **Registered User** radio button.
7. Enter **admin** for the name and the router admin password for the password and click the **Connect** button.
   A list of USB devices connected to your router displays.
8. From the **Apple** menu, select **System Preferences**.
   The System Preferences window displays.
9. Select **Time Machine**.
   The Time Machine window displays.
10. Click the **Select Backup Disk** button and select your USB HDD from the list.
11. 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.

12. When prompted, select the **Registered User** radio button.
13. Enter **admin** for the name and the router admin password for the password and 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 manage the methods that give access to a USB storage device that is connected to the router.

To specify the storage device access settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **Settings > USB Storage > ReadySHARE Storage**.
   The USB Storage (Advanced Settings) page displays.

5. To specify a name for the workgroup that the USB device or devices are members 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.

   The router supports the following access methods:

   - **Network Neighborhood/MacShare**. Access is enabled by default and no password is required. To access the USB storage device within your network, type **\\readyshare**.
   - **HTTP**. Access is enabled by default and no password is required. To access the USB storage device within your network, type **http://readyshare.routerlogin.net/shares**. You can also click the link that is shown in the Link column.
     The fixed port is number is 80.
   - **HTTPS (via internet)**. Access is disabled by default. If you enable this feature, by default, a password is required. To access the USB storage device remotely over the Internet, type **https://***<public IP address>***/shares**. *<public IP address>* is the external or public IP address that is assigned to the router (for example, 1.1.10.102). You can also click the link that is shown in the Link column.
     This feature supports file uploading only. The default port is number 443, which you can change.
   - **FTP**. Access is disabled by default. If you enable this feature, by default, no password is required. To access the USB storage device within your network and download or upload files, type **ftp://readyshare.routerlogin.net/shares**. You can also click the link that is shown in the Link column.
     The fixed port is number is 21.
   - **FTP (via internet)**. Access is disabled by default. If you enable this feature, by default, a password is required. To access the USB storage device remotely over the Internet, type **ftp://***<public IP address>***/shares**. *<public IP address>* is the external or public IP address that is assigned to the router (for example, 1.1.10.102). You can also click the link that is shown in the Link column.
     The default port is number 21, which you can change.
     If you set up Dynamic DNS (see Set up and manage Dynamic DNS on page 156), 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 device over the Internet and download or upload files.

6. For any access method, to allow access, the select associated **Enable** check box.
   To prevent access, clear the associated **Enable** check box.
7. For any access method, to require access with the same password that you specified the first time that you logged in to the router, select the associated **Admin Password Protection** check box.
   To remove the password requirement, clear the associated **Admin Password Protection** check box.
8. Click the **Apply** button.
   Your settings are saved.

Use FTP within the network

File Transfer Protocol (FTP) lets you send and receive large files faster.

To set up FTP access:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > USB Storage > ReadySHARE Storage**.
   The USB Storage (Advanced Settings) page displays.
5. Select the **FTP** check box.
6. Click the **Apply** button.
   Your settings are saved.

Manage network folders on a USB storage device

From a computer or device on the network, you can view, add, or change network folders on a USB storage device that is connected to a USB port on the router.

View network folders on a USB storage device

You can view the network folders on a storage device connected to the router.

To view network folders:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > USB Storage > ReadySHARE Storage**.
   The USB Storage (Advanced Settings) page displays.
5. Scroll down to the Available Networks Folder section to view the following settings:
   The Available Networks Folder section shows the following information for an attached USB device:
   - **Share Name**. The default share name is USB_Storage (as in \\readyshare\USB_Storage).
   - **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 router.
   - **Folder Name**. The full path of the network folder.
   - **Volume Name**. The volume name from the storage device.
   - **Total Space and Free Space**. Show the current utilization of the storage device.

Add a network folder on a USB storage device

You can add network folders on a USB storage device that is connected to a router USB port.

To add a network folder:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > USB Storage > ReadySHARE Storage**.
   The USB Storage (Advanced Settings) page displays.
5. In the Available Network Folders section, select the USB storage device.
6. 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.
7. Complete the fields.

   Note: For read access and write access, the user name (account name) for All–no password is guest. The password for admin is the same one that you use to log in to the router.

8. Click the **Apply** button.
   The folder is added on the USB storage device and the Create Network Folder window closes.

Change a network folder on a USB storage device

You can change network folders on a USB storage device that is connected to a router USB port.

To change a network folder:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > USB Storage > ReadySHARE Storage**.
   The USB Storage (Advanced Settings) page displays.
5. In the Available Network Folders section, select the USB storage device.
6. Click the **Edit** button.
   The Edit Network Folder window opens.
7. Change the settings in the fields as needed.
8. Click the **Apply** button.
   Your settings are saved and the Edit Network Folder window closes.

Approve USB devices

For more security, you can set up the router to share only USB devices that you approve.

To approve USB devices to connect to the router and allow only those devices to connect to the router:

1. Make sure that the USB device that you want to approve is attached to the router.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.
   A login window opens.
4. Enter the router user name and password.

The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard displays.

5. Select **Settings > USB Storage > 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.

6. Click the **Approved Devices** button.
   The USB Drive Approved Devices page displays.

7. In the Available USB Devices table, select the USB device that you want to approve.
   If a single USB device is attached to the router, the radio button is selected automatically.

8. Click the **Add** button.
   The USB device is added to the Approved USB Devices table.

9. Select the **Allow only approved devices** check box.
10. Click the **Apply** button.
    Your settings are saved.

    Note: To approve another USB device that is not attached to a USB port, first remove the attached USB device from the USB port (see Safely remove a USB storage device on page 153), attach the other USB device, and repeat this procedure.

Safely remove a USB storage device

Before you physically disconnect a USB storage device from the router USB port, log in to the router and take the USB storage device offline.

To remove a USB storage device safely:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.

3. Enter the router admin user name and password.

The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard displays.

4. Select **Settings > USB Storage > ReadySHARE Storage**.
   The USB Storage (Advanced Settings) page displays.
5. In the Available Network Folders sections, select the USB storage device.
6. Click the **Safely Remove USB Device** button.
   The router takes the device offline.
7. Physically disconnect the USB storage device.

11

Use Dynamic DNS to Access USB Storage Devices Through the Internet

With Dynamic DNS, you can use the Internet to access USB storage devices that are attached to the router's USB ports when you are not home.

This chapter includes the following sections:

Set up your personal FTP server

With a customized free URL, you can use FTP to access your network when you are not home through Dynamic DNS. Before you set up your FTP server, register for a NETGEAR Dynamic DNS (DDNS) service account and specify the account settings.

Note: The router supports only basic DDNS, and the login and password might not be secure. You can use DDNS with a VPN tunnel for a secure connection.

The following procedure describes the high-level steps that are required to set up a personal account and use FTP. The procedures in this chapter provide details.

To set up your personal account and use FTP:

1. Get your NETGEAR Dynamic DNS domain name.
   For more information, see Set up a new Dynamic DNS account on page 157.
2. Make sure that your Internet connection is working.
   Your router must use a direct Internet connection. It cannot connect to a different router to access the Internet.
3. Connect a storage device to the router.
4. 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 router.
   When you connect the USB storage device to the router 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 on your local area network (LAN).
5. Set up FTP access in the router.
   See Set up FTP access through the Internet on page 161.
6. On a remote computer with Internet access, you can use FTP to access your router by using ftp://*MyName*.mynetgear.com.
   See Use FTP to access storage devices through the Internet on page 162.

Set up and manage Dynamic DNS

Internet service providers (ISPs) assign numbers called 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 don't know what their IP addresses are or when this number changes.

To make it easier to connect, you can get a free account with a Dynamic DNS service that lets you use a domain name to access your home network. To use this account, you must set up the router to use Dynamic DNS. Then the router notifies the Dynamic DNS service provider whenever its IP address changes. When you access your Dynamic DNS account, the service finds the current IP address of your home network and automatically connects you.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

Set up a new Dynamic DNS account

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Dynamic DNS**.
   The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select **NETGEAR**.
   You can select another service provider.
7. Select the **No** radio button.
8. In the **Host Name** field, type the name that you want to use for your URL.
   The host name is sometimes called the domain name. Your free URL includes the host name that you specify and ends with mynetgear.com. For example, specify *MyName*.mynetgear.com.
9. In the **Email** field, type the email address for your account.
10. In the **Password (6-32 characters)** field, type the password for your account.
11. To agree to the terms of service, select the check box.

12. Click the **Register** button.
13. Follow the instructions on the page to register for your NETGEAR Dynamic DNS service.

Specify a DNS account that you already created

If you already created a Dynamic DNS account with NETGEAR, No-IP, or DynDNS, you can set up the router to use your account.

To set up Dynamic DNS if you already created an account:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Dynamic DNS**.
   The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select your provider.
7. Select the **Yes** radio button.
   The page adjusts and displays the **Show Status**, **Cancel**, and **Apply** buttons.
8. In the **Host Name** field, type the host name (sometimes called the domain name) for your account.
9. For a No-IP or DynDNS account, in the **User Name** field, type the user name for your account.
10. For a NETGEAR account at No-IP, in the **Email** field, type the email address for your account.
11. In the **Password (6-32 characters)** field, type the password for your DDNS account.
12. Click the **Apply** button.
    Your settings are saved.
13. To verify that your Dynamic DNS service is enabled in the router, click the **Show Status** button.

A message displays the Dynamic DNS status.

Change the Dynamic DNS settings

You can change the settings for your Dynamic DNS account.

To change your settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Dynamic DNS**.
   The Dynamic DNS page displays.
5. Change your DDNS account settings as necessary.
6. Click the **Apply** button.
   Your settings are saved.

Access USB storage devices through the Internet

If you connect a USB storage device to the router, you can access the USB device through the Internet when you are not home. After you gain access, you can use FTP to share files on the USB device.

Set up HTTPS access through the Internet

To set up HTTPS access through the Internet:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.

3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **Settings > USB Storage > ReadySHARE Storage**.
   The USB Storage (Advanced Settings) page displays.
5. Select the **HTTPS (via Internet)** check box.
   The default port is number 443. Password protection is enabled by default. We recommend that you keep password protection enabled.
6. Click the **Apply** button.
   Your settings are saved.
   The link that lets you access the device over the Internet is https://*public-ip-address*/shares. In this link, *public-ip-address* represents one of the following:
   - The IP address that is assigned to the router's Internet port. You can view this IP address on the ADVANCED Home page.
   - If you set up a DDNS account, the router's DNS name, for example, *yourname.mynetgear.com*.
7. To limit read and write access of a device to the admin user, select a device in the Available Network Folder's section.
   If only one device is connected, it is automatically selected.
8. Click the **Edit** button.
   The Edit page displays.
9. From the **Read Access** menu, select **admin**.
10. From the **Write Access** menu, select **admin**.
11. Click the **Apply** button.
    Your settings are saved.

Access USB storage devices from a remote computer

To access USB storage devices from a remote computer:

1. Launch a web browser on a computer that is not on your home network.
2. Connect to your home router:

- To connect with Dynamic DNS, type the DNS name.
  To use a Dynamic DNS account, you must enter the account information on the Dynamic DNS page. See Set up and manage Dynamic DNS on page 156.
- To connect without Dynamic DNS, type the router's Internet port IP address.
  You can view the router's Internet IP address on the router's System Information page.

Set up FTP access through the Internet

To set up FTP access over the Internet:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > USB Storage > ReadySHARE Storage**.
   The USB Storage (Advanced Settings) page displays.
5. Select the **FTP (via internet)** check box.
6. Click the **Apply** button.
   Your settings are saved.
7. To limit access to the admin user, in the Available Network Folder section, select the USB storage device.
   If only one device is connected, it is automatically selected.
8. Click the **Edit** button.
   The Edit Network Folder window opens.
9. From the **Read Access** menu, select **admin**.
10. From the **Write Access** menu, select **admin**.
11. Click the **Apply** button.
    Your settings are saved and the Edit Network Folder window closes.

Use FTP to access storage devices through the Internet

If you attached a storage device to the router, before you can access the storage device through the Internet with FTP, you must first set it up (see Set up FTP access through the Internet on page 161).

To access a USB 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 router, launch a web browser.
   - To upload a file to a storage device connected to the 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**.

   If you are using Dynamic DNS, your domain name is MyName, and you use the NETGEAR DDNS server, type the DNS name **ftp://MyName.mynetgear.com**.
3. When prompted, log in:
   - To log in as admin, in the **user name** field, enter **admin** and in the **password** field, enter the same password that you use to log in to the router.
   - To log in as guest, in the **user name** field, enter **guest**.

   The guest user name does not need a password.

   The files and folders that your account can access on the USB device display. For example, you might see `share/partition1/directory1`.
4. Navigate to a location on the USB device.
5. Download or upload the file.

12

Use the Router as a Media Server

The router comes set up to work as a ReadyDLNA media server. You can set up the router to play music from iTunes server and media from TiVo.

This chapter contains the following sections:

Specify ReadyDLNA media server settings

By default, the router functions as a ReadyDLNA media server, which lets you view movies and photos on DLNA/UPnP AV–compliant media players, such as Xbox360, Playstation, and NETGEAR media players.

To specify media server settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > USB Storage > Media Server**.
   The Media Server (Settings) page displays.
5. Specify the following settings:
   - **Enable DLNA Media Server**. By default, this check box is selected to enable the router to function as a media server. You can clear the check box to disable the media server functionality.
   - **Enable TiVo support**. By default, this check box is selected so that you can play ReadyNAS media on your TiVo device. You can clear the check box to disable TiVo support.
     For more information, see Set up the router to work with TiVo on page 167.
   - **Enable iTunes Server (Music Only)**. Select this check box to play music from a USB device that is connected to your router with iTunes on your Windows-based or Mac computer using Home Sharing.
     For more information, see Play music from a storage device with iTunes server on page 165.
   - **Media Server Device Name**. The default media server device name is ReadyDLNA:XR500. To change the router device name, which affects the XR500 extension of the media server device name, click the **Edit** button. Changing the router device name also affects the storage folder name.
6. Click the **Apply** button.
   Your settings are saved.

The router automatically scans for media files when new files are added to your ReadySHARE USB storage device. The router can scan only shared folders that do not require a password.

7. To scan for new media files immediately, click the **Rescan media files** button.

Play music from a storage device with iTunes server

iTunes server lets you play music from a USB storage device that is connected to a USB port on your router with iTunes on your Windows-based or Mac computer or with the iTunes Remote app on your iPhone or iPad. You can also use the iTunes 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 router's iTunes server with iTunes

You can play music from a USB storage device that is connected to your router with iTunes on your Windows-based or Mac computer using Home Sharing. To set up Home Sharing, you need an Apple account and the latest version of iTunes installed on your computer.

To set up the router's iTunes server to play music on iTunes:

1. Connect a USB storage device to a USB port on your 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 router.

   When you connect the USB storage device to the 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 on your local area network (LAN).
3. Launch a web browser from a computer or mobile device that is connected to the router network.
4. Enter **http://www.routerlogin.net**.

   A login window opens.
5. Enter the router admin user name and password.

The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The Dashboard displays.

6. Select **Settings > USB Storage > Media Server**.
   The Media Server (Settings) page displays.
7. Select the **Enable iTunes Server (Music Only)** check box.
8. Click the **Apply** button.
   Your settings are saved.
9. On your Windows-based or Mac computer, launch iTunes.
10. Select **File > Home Sharing > Turn On Home Sharing**.
    The Home Sharing page displays.
11. Enter your Apple ID email address and password.
12. Click the **Turn On Home Sharing** button.
    When Home Sharing is enabled, a **Home Sharing** icon displays in iTunes.
13. Click the **Home Sharing** icon, and from the menu, select the router.
    The music that is on the USB device that is connected to the router displays in iTunes.

Set up the router's iTunes server with the iTunes Remote app

You can play music from a USB storage device that is connected to your router on your iPhone or iPad using the iTunes Remote app.

To set up the router's iTunes server to play music on your iPhone or iPad:

1. Connect a USB storage device to a USB port on your 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 router.

   When you connect the USB storage device to the 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 on your local area network (LAN).
3. Connect your iPhone or iPad to your router's WiFi network.
4. Download the iTunes Remote app from the Apple App Store.

5. Launch the iTunes Remote app from your iPhone or iPad.
6. In the iTunes Remote app, click the **Add a Device** button.
   The passcode displays in the app.
7. Specify the passcode in the router to set up your iTunes server:
   a. Launch a web browser from a computer or mobile device that is connected to the router network.
   b. Enter **http://www.routerlogin.net**.
      A login window opens.
   c. Enter the router admin user name and password.
      The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
      The Dashboard displays.
   d. Select **Settings > USB Storage > Media Server**.
      The Media Server (Settings) page displays.
   e. Select the **Enable iTunes Server (Music Only)** check box.
   f. Click the **Apply** button.
      Your settings are saved.
   g. Enter the passcode.
   h. Click the **Allow Control** button.
      Your passcode is saved.
      Your iPhone or iPad pairs with the router and the iTunes Server is ready. The router displays in the Remote app.
8. In the iTunes Remote app, tap the router that your iPhone or iPad is connected to.
   The music that is on the USB storage device that is connected to the router displays in the app.

Set up the router to work with TiVo

You can set up your TiVo to access media files stored on a USB storage device that is connected to your router. The TiVo must be on the same network as the 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 or Mac computer in your TiVo user interface.

To set up the router to work with TiVo:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > USB Storage > Media Server**.
   The Media Server (Settings) page displays.
5. Make sure that the **Enable TiVo support** check box is selected.
6. If you changed the settings, click the **Apply** button.
   Your settings are saved.

13

Share a USB Printer

The ReadySHARE Printer utility lets you share a USB printer that is connected to a USB port on your router. You can share this USB printer among the Windows-based and Mac computers on your network.

For more information about the features available in the NETGEAR USB Control Center, see the *ReadySHARE Printer User Manual*, which is available at http://downloadcenter.netgear.com.

This chapter contains the following sections:

Install the printer driver and cable the printer

Some USB printer manufacturers (for example, HP and Lexmark) request that you do not connect the USB cable until the installation software prompts you to do so.

To install the driver and cable the printer:

1. On each computer on your network that shares the USB printer, install the driver software for the USB printer.

   If you cannot locate the printer driver, contact the printer manufacturer.

2. Use a USB printer cable to connect the USB printer to a router USB port.

Download the ReadySHARE printer utility

The utility works on Windows-based and Mac computers.

To download the utility:

1. Visit https://www.netgear.com/home/discover/apps/readyshare.
2. Click the **PRINT - Learn how you can print wirelessly from many devices** link.
3. Click the **Download PC installer and get started link** to download the ReadySHARE Printer utility setup file to your Windows-based computer.
4. Follow the instructions on the page to download the ReadySHARE Printer utility.

Install the ReadySHARE printer utility

You must install the ReadySHARE Printer utility on each computer that will share the printer. After you install it, the utility displays as NETGEAR USB Control Center on your computer. For more information about how to use the NETGEAR USB Control Center, visit https://www.netgear.com/support/product/ReadySHARE_USB_Printer.aspx.

To install the utility:

1. If necessary, unzip the ReadySHARE Printer utility setup file.
2. Double-click the ReadySHARE Printer utility setup file that you downloaded.

   The InstallShield Wizard opens.

3. Follow the prompts to install the NETGEAR USB Control Center.

   After the InstallShield Wizard completes the installation, the NETGEAR USB Control Center prompts you to select a language.

4. Select a language from the menu and click the **OK** button.
   The NETGEAR USB Control Center opens.

   Some firewall software, such as Comodo, blocks the NETGEAR USB Control Center from accessing the USB printer. If you do not see the USB printer displayed on the page, you can disable the firewall temporarily to allow the utility to work.

5. Select the printer and click the **Connect** button.
   The printer status changes to Manually connected by *Mycomputer*. Now only the computer that you are using can use this printer.

6. Click the **Disconnect** button.
   The status changes to Available. Now all computers on the network can use the printer.

7. To exit the utility, select **System > Exit**.

Print using the NETGEAR USB Control Center

For each computer, after you click the **Connect** and **Disconnect** buttons once, the utility automatically manages the printing queue. By default, the utility starts automatically whenever you log on to Windows and runs in the background.

To print a document using the NETGEAR USB Control Center:

1. Click the **NETGEAR USB Control Center** icon .
   The NETGEAR USB Control Center page displays.

2. Select a printer and click the **Connect** button.
   The printer status changes to Manually connected by *Mycomputer*. Now only the computer that you are using can use this printer.

3. Use the print feature in your application to print your document.
   The NETGEAR USB Control Center automatically connects your computer to the USB printer and prints the document. If another computer is already connected to the printer, your print job goes into a queue to wait to be printed.

4. If your document does not print, use the NETGEAR USB Control Center to check the printer status.
5. To release the printer so that all computers on the network can use it, click the **Disconnect** button.

The status changes to Available. Now any computers on the network can use the printer.

6. To exit the utility, select **System > Exit**.

14

Use OpenVPN to Access Your Network

You can use OpenVPN software to remotely access your router with virtual private networking (VPN). This chapter explains how to install and use OpenVPN software to set up a VPN tunnel.

The chapter contains the following sections:

About VPN connections

A virtual private network (VPN) lets you use the Internet to securely access your network when you aren't home.

This type of VPN access is called a client-to-gateway tunnel. The computer is the client, and the router is the gateway. To use the VPN feature, you must do the following:

- Log in to the router to enable and configure OpenVPN (see Enable OpenVPN service in the router on page 175).
- Install OpenVPN client software and configuration files on your device from which you want to use VPN (see Install OpenVPN software on a VPN client on page 176).
- Run the OpenVPN client software on your device when you want to use a VPN connection.

Enabling OpenVPN on your router allows VPN connections between the router and a client, for example your laptop when you are away from home. The router provides the VPN service and the laptop is the VPN client. Traffic between the router and the laptop is encrypted.

Note: The router itself does not function as a VPN client to an external VPN service provider, so it does not encrypt traffic passing between your home network and the Internet.

VPN can use either Dynamic DNS (DDNS) or a static IP address to connect with your router:

- To use a DDNS service, register for a DDNS account with a host name. You use the host name to access your network. The router supports these DDNS accounts: NETGEAR, No-IP, and Dyn. For more information, see Set up and manage Dynamic DNS on page 156.
- If your Internet service provider (ISP) assigned a static WAN IP address that never changes, the VPN can use that IP address to connect to your home network.

Enable OpenVPN service in the router

You must enable the OpenVPN service settings in the router before you can use a VPN connection.

To enable OpenVPN service:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Settings > VPN Service**.
   The VPN page displays.

   Note: The OpenVPN configuration software packages that you can download on the page are for the VPN client devices (see Install OpenVPN software on a VPN client on page 176).
5. Select the **Enable VPN Service** check box.
   We recommend that you use the default TUN mode and TAP mode settings. (These settings determine how VPN information is transferred.) If you know that you need other settings, you can change the TUN mode and TAP mode settings, but you must do so *before* you download and install the OpenVPN configuration software packages on client devices (see Install OpenVPN software on a VPN client on page 176).
6. To change the TUN mode settings, do the following:
   - To change the TUN mode service type, select the **UDP** or **TCP** radio button. The default protocol for TUN mode is UDP.
   - To change the TUN mode service port, type the port number that you want to use in the field.
     The default port number for TUN mode is 12973. The TUN port number is used in the `.ovpn` file of the OpenVPN configuration software package for Mac and non-Windows clients.

7. To change the TAP mode settings, do the following:
   - To change the TAP mode service type, select the **UDP** or **TCP** radio button. The default protocol for TAP mode is UDP.
   - To change the TAP mode service port, type the port number that you want to use in the field.
     The default port number for TAP mode is 12974. The TAP port number is used in the `.ovpn` file of the OpenVPN configuration software package for Windows clients.

8. Click the **Apply** button.
   Your changes are saved. VPN is enabled in the router, but you must install and set up OpenVPN software on your device before you can use a VPN connection.

Install OpenVPN software on a VPN client

You must install OpenVPN software on each Windows-based computer, Mac computer, iOS device, and Android device that you plan to use for VPN connections to your router. Each computer or device is called a VPN client.

The software consists of the application software and the configuration files:

- Download and install the application software from the link that is provided in each client-specific section.
- Download and install the configuration files from the router as described in each client-specific section. The configuration files provide the correct router configuration information for the client utility. You must download the configuration files *after* you enable and configure OpenVPN service in the router (see Enable OpenVPN service in the router on page 175).

  Note: If you later change the OpenVPN configuration in the router (for example, you change the TUN or TAP port number), you must download and install the `.ovpn` configuration file again on each client, depending on its operating system. If you change the TUN port number in the router, the `.ovpn` configuration file for Mac and non-Windows clients changes. If you change the TAP port number in the router, the `.ovpn` configuration file for Windows clients changes.

Install OpenVPN software on a Windows-based computer

You must install both the OpenVPN client utility and OpenVPN configuration files on each Windows-based computer where you want to use a VPN connection to your router.

To download and install the OpenVPN client utility and OpenVPN configuration files on a Windows-based computer:

1. To download the OpenVPN client utility on your Windows-based computer, visit openvpn.net/community-downloads/.
2. Select the Windows package with the installer files.

   In most situations, you can download the Windows 32-bit or Windows 64-bit installer files, depending on your Windows operating system.
3. Download and install the OpenVPN client utility on your computer.

   You need to have administrative privileges.
4. Launch a web browser from the computer, which must be connected to the router network.
5. Enter **http://www.routerlogin.net**.

   A login window opens.
6. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The BASIC Home page displays.
7. Select **ADVANCED > Advanced Settings > VPN Service**.

   The VPN Service page displays.
8. Make sure that the **Enable VPN Service** check box is selected.

   For more information about the VPN configuration for the router, see Enable OpenVPN service in the router on page 175.
9. Click the **For Windows** button to download the router's OpenVPN configuration files to your Windows-based computer.
10. Unzip the OpenVPN configuration files and copy them to the folder in which you installed the OpenVPN client utility.
11. Modify the VPN interface name to **NETGEAR-VPN**:
    a. If your computer is running Windows 10, select **Control Panel > Network and Sharing Center > Change adapter settings**.

       If your computer is running another Windows version, find the page that lets you change the adapter settings.

    b. In the local area connection list, find the local area connection with the device name **TAP-Windows Adapter**.

c. Select the local area connection and change its name (*not* its device name) to **NETGEAR-VPN**.

   If you do not change the VPN interface name, the VPN tunnel connection will fail.

You can now open a VPN tunnel to the router.

For more information about installing and using OpenVPN on your Windows-based computer, visit https://openvpn.net/community-resources/how-to/#quick.

Install OpenVPN software on a Mac computer

You must install both the Tunnelblick OpenVPN client utility and OpenVPN configuration files on each Mac computer where you want to use a VPN connection to your router.

To download and install the Tunnelblick OpenVPN client utility and OpenVPN configuration files on a Mac computer:

1. To download the Tunnelblick OpenVPN client utility on your Mac computer, visit https://tunnelblick.net/downloads.html.
2. Download and install the Tunnelblick OpenVPN client utility on your Mac computer.

   You need to have administrative privileges.
3. Launch a web browser from the Mac computer, which must be connected to the router network.
4. Enter **http://www.routerlogin.net**.

   A login window opens.
5. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The BASIC Home page displays.
6. Select **ADVANCED > Advanced Settings > VPN Service**.

   The VPN Service page displays.
7. Make sure that the **Enable VPN Service** check box is selected.

   For more information about the VPN configuration for the router, see Enable OpenVPN service in the router on page 175.
8. Click the **For Mac OS X** button to download the router's OpenVPN configuration files to your Mac computer.
9. Unzip the OpenVPN configuration files and copy them to the folder in which you installed the Tunnelblick OpenVPN client utility.

You can now open a VPN tunnel to the router.

For more information about installing and using OpenVPN on your Mac computer, visit https://openvpn.net/vpn-server-resources/installation-guide-for-openvpn-connect-client-on-macos/.

Install OpenVPN software on an iOS device

You must install both the OpenVPN Connect app and OpenVPN configuration files on each iOS device where you want to use a VPN connection to your router.

To download and install the OpenVPN Connect app and OpenVPN configuration files on an iOS device:

1. On your iOS device, download and install the OpenVPN Connect app from the Apple app store.
2. Launch a web browser from a computer or your iOS device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.

   A login window opens.
4. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The BASIC Home page displays.
5. Select **ADVANCED > Advanced Settings > VPN Service**.

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

   For more information about the VPN configuration for the router, see Enable OpenVPN service in the router on page 175.
7. Click the **For Smart Phone** button to download the router's OpenVPN configuration files to your computer or iOS device.

   If you download the configuration files to your computer, unzip the files, and send them your iOS device.
8. On your iOS device, do the following:
   a. Open the `.ovpn` file.
   b. If the OpenVPN Connect app does not start automatically, a list of apps might display: Select the OpenVPN Connect app.
   c. Install the `.ovpn` file.

You can now open a VPN tunnel to the router.

For more information about installing and using OpenVPN on your iOS device, visit https://www.vpngate.net/en/howto_openvpn.aspx#ios.

Install OpenVPN software on an Android device

You must install both the OpenVPN Connect app and OpenVPN configuration files on each Android device where you want to use a VPN connection to your router.

To download and install the OpenVPN Connect app and OpenVPN configuration files on an Android device:

1. On your Android device, download and install the OpenVPN Connect app from the Google Play Store.
2. Launch a web browser from a computer or your Android device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.

   A login window opens.
4. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The BASIC Home page displays.
5. Select **ADVANCED > Advanced Settings > VPN Service**.

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

   For more information about the VPN configuration for the router, see Enable OpenVPN service in the router on page 175.
7. Click the **For Smart Phone** button to download the router's OpenVPN configuration files to your computer or Android device.

   If you download the configuration files to your computer, unzip the files, and send them your Android device.
8. On your Android device, open the `.ovpn` file and import it into the OpenVPN Connect app.

You can now open a VPN tunnel to the router.

For more information about using OpenVPN on your Android device, visit https://www.vpngate.net/en/howto_openvpn.aspx#android.

LAN IP addressing in VPN networks

For the VPN connection to work, your computer or device (the VPN client) must be connected to a network that uses a different LAN IP address scheme than your router.

The default LAN IP address scheme for the router is 192.168.1.x. (The most common IP schemes are 192.168.x.x, 172.x.x.x, and 10.x.x.x.) If you experience a conflict, change the IP scheme either for your home network or for the network where your VPN client device is connected.

If both networks use the same LAN IP scheme, when the VPN tunnel is established, you cannot access your home router or your home network with the OpenVPN software.

For information about changing the LAN settings on the router, see Change the router's LAN IP address and RIP settings on page 85.

Use VPN to remotely access a USB storage device attached to the router

If you attach a USB storage device to a USB port on your router, after you make a VPN connection from a remote VPN client device to your home router, you can access the USB storage device. Because the router supports ReadySHARE, the USB storage device might display as a ReadySHARE network device on your home router's local LAN.

Note: On the remote VPN client, your home router might display as the remote router.

Use VPN to access your Internet service at home

When you're away from 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.

Your router lets you use a VPN connection to access your own Internet service when you're away from home. You might want to do this if you travel to a geographic location that doesn't support all the Internet services that you use at home. For example, your Netflix account might work at home but not in a different country.

Allow VPN client Internet access in the router

By default, the router is set up to allow VPN connections only to your home network, but you can change the settings to allow Internet access. Accessing the Internet remotely through a VPN might be slower than accessing the Internet directly.

To allow VPN clients to use your home Internet service:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Settings > VPN Service**.
   The VPN Service page displays.
5. Make sure that the **Enable VPN Service** check box is selected.
   For more information about the VPN configuration for the router, see Enable OpenVPN service in the router on page 175.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **All sites on the Internet & Home Network** radio button.
   When you access the Internet with the VPN connection, instead of using a local Internet service, you use the Internet service from your home network.
7. Click the **Apply** button.
   Your settings are saved.

Block VPN client Internet access in the router

By default, the router is set up to allow VPN connections only to your home network, not to the Internet service for your home network. If you changed this setting to allow Internet access, you can change it back.

To allow VPN clients to access only your home network and block them from using the Internet service for your home network:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Settings > VPN Service**.
   The VNP page displays.
5. Make sure that the **Enable VPN Service** check box is selected.
   For more information about the VPN configuration for the router, see Enable OpenVPN service in the router on page 175.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **Home Network only** radio button.
   This is the default setting. The VPN connection is only to your home network, not to the Internet service for your home network.
7. Click the **Apply** button.
   Your settings are saved.

15

Use VPN to Access An External Network

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

For information about using the router as a VPN server, see Use OpenVPN to Access Your Network on page 173.

This chapter includes the following sections:

Set up a VPN client connection

In addition to using a virtual private network (VPN) to securely access your own network over the Internet when you are not home (see Use OpenVPN to Access Your Network on page 173), you can also set up the router as a VPN client to let devices on the router's network securely access an *external* network, while protection your own network identity and preventing a distributed denial-of-service (DDoS) attack. An external network can be a gaming network, a business network behind a firewall, or an Internet service that might not be accessible from your geographical location without using a VPN server in another country.

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

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

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

To use the VPN client feature, you must log in to the router, enable the router's VPN client, and establish a connection to an external VPN server (see Enable the VPN client in the router and connect to a VPN server on page 185).

Enable the VPN client in the router and connect to a VPN server

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

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

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > VPN Client**.
   The VPN Client page displays.
5. Select the **Enable VPN Client** check box.
   The VPN settings on the page becomes available.
6. If you do not own a license a predefined VPN services, do the following:
   a. From the **VPN Server** menu, select a VPN provider.
   b. Click the **Buy a License** link.
      A provider web page opens that lets you choose a price plan and purchase a license.
   c. Follow the instructions on the web page.
   d. When you obtain a license, write down your user name and password for the VPN service.
7. From the **VPN Server** menu, select a VPN provider.
   The option is HideMyAss.
8. From the **VPN Protocol** menu, select **UDP** or **TCP**.
   UDP functions without error correction in transmission, so it is faster, but less reliable. TCP functions with error correction in transmission, so it is more reliable, but slower.
9. From the **Country** menu, select the country in which you want to use the VPN server.
10. From the **City** menu, select the city in which you want to use the VPN server.
11. In the **Username** field, enter the user name for authentication with the VPN server.
12. In the **Password** field, enter the password for authentication with the VPN server.

13. Click the **Connect** button.

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

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

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

    - **Connecting**. The router is attempting to connect to the VPN server.
    - **Connected**. The router is connected to the VPN server.
    - **Disconnected**. The router is connected to the VPN server.
    - **Error**. The connection to the VPN server failed.
      If you experience difficulty in establishing a VPN connection, click the **Show Logs** link and see if any log messages provide helpful information. For more information about the logs, see . on page 133.

Disconnect the router from the VPN server

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

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > VPN Client**.

   The VPN Client page displays.
5. Click the **Disconnect** button.

   The VPN connection is terminated.

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

16

Manage and Customize Internet Traffic Rules for Ports

You can use port forwarding and port triggering to set up rules for Internet traffic. You need networking knowledge to set up these features.

This chapter includes the following sections:

Manage port forwarding to a local server for services and applications

If your home network includes a server, 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 router can forward incoming traffic with specific protocols to computers on your local network. You can specify the servers for services and applications and you can also specify a default DMZ server to which the router forwards all other incoming protocols (see Set up a default DMZ server on page 83).

Set up port forwarding to a local server

The router comes with default port forwarding services and applications. 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.

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

   The computer that functions as the server must always use the same IP address.

3. Assign the server computer a reserved IP address.

   For more information, see Manage reserved LAN IP addresses on page 88.

4. Launch a web browser from a computer or mobile device that is connected to the router network.
5. Enter **http://www.routerlogin.net**.

   A login window opens.

6. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.

7. Select **Settings > Advanced Settings > Port Forwarding**.

   The Port Forwarding page displays.

8. From the **Service Name** menu, select the service name.
   If the service that you want to add is not in the menu, create a custom service. See Add a custom port forwarding service or application on page 190.
9. In the **Server IP Address** field, enter the IP address of the computer that must provide the service.
10. Click the **Add** button.
    Your settings are saved and the service or application is added to the table.

Add a custom port forwarding service or application

The router comes with default services and applications that you can use for port forwarding. If the service or application is not predefined, you can add a custom port forwarding service or application.

To add a custom service or application:

1. Find out which port number or range of numbers the application uses.
   You can usually find this information by contacting the publisher of the application or user groups or news groups.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.
   A login window opens.
4. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
5. Select **Settings > Advanced Settings > Port Forwarding**.
   The Port Forwarding page displays.
6. Click the **Add Custom Service** button.
   The Ports - Custom Services page displays.
7. In the **Service Name** field, enter a descriptive name.
8. From the **Protocol** menu, select the protocol.
   If you are unsure, select **TCP/UDP**.
9. In the **External port range** field, type the port numbers and port ranges.

Divide ports and port ranges by commas and hyphens, for example, 20, 40-50, 34700-34710.

10. Specify the internal ports by one of these methods:
    - Leave the **Use the same port range for Internal port** check box selected.
    - Type the port numbers and port ranges in the **Internal port range** field, dividing ports and port ranges by commas and hyphens, for example, 30, 50-60, 65500-65510.
11. In the **Internal IP address** field, type the IP address or select the radio button for an attached device listed in the table.
12. Click the **Apply** button.

    Your settings are saved. The service or application is added to the table on the Port Forwarding page.

Change a port forwarding service or application

To change a port forwarding service or application:

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

   A login window opens.
3. Enter the router user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > Port Forwarding**.

   The Port Forwarding page displays.
5. In the table, select the radio button next to the name of the service or application.
6. Click the **Edit Service** button.

   The Ports - Custom Services page displays.
7. Change the settings.

   For information about the settings, see Add a custom port forwarding service or application on page 190.
8. Click the **Apply** button.

   Your settings are saved.

Remove a port forwarding service or application

To remove a port forwarding service or application:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Port Forwarding**.
   The Port Forwarding page displays.
5. In the table, select the radio button next to the name of the service or application.
6. Click the **Delete Service** button.
   The service or application is removed.

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 router always gives your web server an IP address of 192.168.1.33.
2. On the Port Forwarding page, configure the router to forward the HTTP service to the local address of your web server at **192.168.1.33**.
   HTTP (port 80) is the standard protocol for web servers.
3. (Optional) Register a host name with a Dynamic DNS service (see Set up and manage Dynamic DNS on page 156) and specify that name on the Dynamic DNS page of the router.

Dynamic DNS makes it much easier to access a server from the Internet because you can type the name in the Internet browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

How the router implements a port forwarding rule

The following sequence shows the effects of a port forwarding rule:

1. When you type 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 router.
   - **Destination port number**. 80, which is the standard port number for a web server process.

   Your router receives the message and finds your port forwarding rule for incoming port 80 traffic.
2. The router changes the destination in the message to IP address 192.168.1.123 and sends the message to that computer.
3. Your web server at IP address 192.168.1.123 receives the request and sends a reply message to your router.
4. Your 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.

Manage port triggering for services and applications

Port triggering is 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 router monitors traffic to the Internet from an outbound "trigger" port that you specify. For outbound traffic from that port, the router saves the IP address of the computer that sent the traffic. The router temporarily opens the incoming port or ports that you specify for your port triggering service or application 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, enable Universal Plug and Play (UPnP). See Improve network connections with Universal Plug and Play on page 97.

Add a port triggering service or application

Unlike port forwarding, the router does not come with default port triggering services or applications. You must add them.

To add a port triggering service or application:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Port Triggering**.
   The Port Triggering page displays.
5. Click the **Add Service** button.
   The Port Triggering - Services page displays.
6. In the **Service Name** field, type a descriptive service name.
7. From the **Service User** menu, select a user option:
   - **Any** (the default) allows any computer on the Internet to use this service.
   - **Single address** restricts the service to a particular computer.
8. From the **Service Type** menu, select **TCP** or **UDP**.
9. In the **Triggering Port** field, enter the number of the outbound traffic port that must open the inbound ports.
10. From the **Connection Type** menu, select **TCP**, **UDP**, or **TCP/UDP** (the default selection).

If you are not sure, leave the **TCP/UDP** selection.

11. In the **Starting Port** and **Ending Port** fields, define the range that the service or application uses by entering the inbound starting port and ending port numbers.
12. Click the **Apply** button.

    Your settings are saved, the page closes, the Port Triggering page displays again, and the service or application is added to the Port Triggering Portmap Table.

    You must make sure that port triggering is enabled before the router can use port triggering. See Enable port triggering and specify the time-out value on page 195.

Enable port triggering and specify the time-out value

After you add one or more port forwarding services or applications (see Add a port triggering service or application on page 194), you can enable port triggering.

To enable port triggering: and specify the time-out value:

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

   A login window opens.
3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

   The Dashboard displays.
4. Select **Settings > Advanced Settings > Port Triggering**.

   The Port Triggering page displays.
5. Make sure that the **Disable Port Triggering** check box is cleared.

   By default, this check box is cleared. If this check box is selected, the router does not use port triggering even if you specified port triggering settings.
6. To change the default time-out value of 20 minutes, in the **Port Triggering Timeout** field, enter a value up to 9999 minutes.

   The time-out value controls how long the inbound ports stay open when the router detects no activity. This value is required because the router cannot detect when the service or application terminates.
7. Click the **Apply** button.

   Your settings are saved.

Change a port triggering service or application

You can change an existing port triggering service or application.

To change a port triggering service or application:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Port Triggering**.
   The Port Triggering page displays.
5. In the Port Triggering Portmap Table, select the radio button next to the service or application name.
6. Click the **Edit Service** button.
   The Port Triggering - Services page displays.
7. Change the settings.
   For information about the settings, see Add a port triggering service or application on page 194.
8. Click the **Apply** button.
   Your settings are saved, the page closes, the Port Triggering page displays again, and the changed service or application displays in the Port Triggering Portmap Table.

Remove a port triggering service or application

You can remove a port triggering service or application that you no longer need.

To remove a port triggering service or application:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.

3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Port Triggering**.
   The Port Triggering page displays.
5. In the Port Triggering Portmap Table, select the radio button next to the service or application.
6. Click the **Delete Service** button.
   The service or application is removed from the Port Triggering Portmap Table.

Disable port triggering

By default, port triggering is enabled. You can disable port triggering temporarily without removing any port triggering services or applications from the Port Triggering Portmap Table.

To disable port triggering:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
4. Select **Settings > Advanced Settings > Port Triggering**.
   The Port Triggering page displays.
5. Select the **Disable Port Triggering** check box.
   By default, this check box is cleared. If this check box is selected, the router does not use port triggering even if you specified port triggering settings.
6. Click the **Apply** button.
   Your settings are saved.

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 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 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 router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your 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 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 router using the NAT-assigned source port (for example, port 33333) as the destination port and sends an "identify" message to your router with destination port 113.
6. When your 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 router restores the original address information replaced by NAT and sends this reply message to your computer.
7. When your 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 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 router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table and incoming traffic is no longer accepted on port numbers 33333 or 113.

17

Troubleshooting

This chapter provides information to help you diagnose and solve problems you might experience with your router. If you do not find the solution here, check the NETGEAR support site at netgear.com/support for product and contact information.

The chapter contains the following sections:

Quick tips

This section describes tips for troubleshooting some common problems.

Sequence to restart your network

If you must restart your network, follow this sequence:

1. Turn off and unplug the modem.
2. Turn off the router.
3. Plug in the modem and turn it on. Wait two minutes.
4. Turn on the router and wait two minutes.

Check the power adapter and Ethernet cable connections

If the router does not start, make sure that the power adapter cable is securely plugged in.

If the Internet connection or LAN connections do not function, make sure that the Ethernet cables are securely plugged in. The Internet LED on the router is lit if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on. If one or more powered-on computers are connected to the router by an Ethernet cable, the corresponding numbered router LAN port LEDs light.

Check the network settings

Be sure that the network settings of your device are correct. Wired devices and devices that are connected over WiFi must use network IP addresses on the same network as the router. The simplest way to do this is to configure each device to obtain an IP address automatically using DHCP.

Some service providers require you to use the MAC address of the device that was initially registered on the account. You can view the MAC address on the Device Manager page (see View and manage devices currently on the network on page 65).

Check the WiFi settings

Be sure that the WiFi settings in your device and the router match exactly. The WiFi network name (SSID) and WiFi security settings of the router and WiFi computer must match exactly.

Troubleshoot with the LEDs

By default, the router is set with standard LED settings.

If you changed the standard LED settings and want to troubleshoot with the LEDs, change the LED settings back to the standard LED settings (see Turn the LEDs on or off using the LED On/Off switch on page 18 or Disable or enable LED blinking or turn off LEDs on page 138).

Standard LED behavior when the router is powered on

After you turn on power to the 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 white.
   - The Internet LED is solid white.
   - The WiFi LED is solid white unless you turned off the WiFi radios.

Power LED is off or blinking

This could occur for a number of reasons. Check the following:

- Make sure that the power adapter is securely connected to your router and securely connected to a working power outlet.
- Make sure that you are using the power adapter that NETGEAR supplied for this product.
- If the Power LED blinks slowly and continuously, the router firmware is corrupted. This can happen if a firmware update is interrupted, or if the router detects a problem with the firmware. If the error persists, it is likely that a hardware problem exists. For recovery instructions, or help with a hardware problem, contact Technical Support at netgear.com/support.

LEDs never turn off

When the router is turned on, the LEDs light for about 10 seconds and then turn off. If all the LEDs stay on, this indicates a fault within the router.

If all LEDs are still lit one minute after power-up, do the following:

- Cycle the power to see if the router recovers.
- Press and hold the **Reset** button to return the router to its factory settings.

If the error persists, a hardware problem might be the cause. Contact Technical Support at netgear.com/support.

Internet or Ethernet port LEDs are off

If you changed the standard LED settings and want to troubleshoot with the LEDs, change the LED settings back to the standard LED settings (see Turn the LEDs on or off using the LED On/Off switch on page 18 or Disable or enable LED blinking or turn off LEDs on page 138).

If either the Ethernet port LEDs or the Internet LED does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.
- Make sure that power is turned on to the connected modem or computer.
- Be sure that you are using the correct cable.

When you connect the router's Internet port to a 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 LEDs are off

If the WiFi LED, 2.4 GHZ LED, 5 GHz LED, and Guest WiFi LED stay off, check to see if someone pressed the **WiFi On/Off** button on the router or if the standard LED settings were changed (see Turn the LEDs on or off using the LED On/Off switch on page 18 or Disable or enable LED blinking or turn off LEDs on page 138).

The WiFi LED, 2.4 GHZ LED, and 5 GHz LED light when the WiFi radios are turned on. However, if the WiFi guest network is disabled in both the 2.4 GHz band and the 5 GHz band, which the default setting, the Guest WiFi LED is off. If the WiFi guest network is enabled in either the 2.4 GHz band or the 5 GHz band, the Guest WiFi LED lights.

You cannot log in to the router

If you are unable to log in to the router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router.
- Make sure that the IP address of your computer is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address is in the range of 192.168.1.2 to 192.168.1.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer 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 computer to the router, and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1.
- 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.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The user name is **admin**, and the password is the one that you specified the first time that you logged in. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services. For example, the router cannot convert ADSL or cable data into Ethernet networking information. NETGEAR does not support such a configuration.

You cannot access the Internet

If you can access your router but not the Internet, check to see if the router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP.

To check the WAN IP address:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Select an external site such as netgear.com.
3. Type **http://www.routerlogin.net**.
   A login window opens.
4. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The Dashboard displays.
5. Select **System Information**.
   The page that displays shows multiple panes.
6. Locate the Internet Status pane and check to see that an IP address is shown in the WAN IP field. If 0.0.0.0 is shown, your router did not obtain an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network. For more information, see Check the Internet connection status, view details, and release and renew the connection on page 136.

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (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 on the Internet Setup page.
- If your ISP allows only one Ethernet MAC address to connect to Internet and checks for your 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 router's MAC address.
  - Configure your router to clone your computer's MAC address.

If your router obtained an IP address, but your computer does not load any web pages from the Internet, it might be for one or more of the following reasons:

- Your computer 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 router's configuration, reboot your computer, and verify the DNS address. You can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- The router might not be configured as the TCP/IP gateway on your computer.
  If your computer obtains its information from the router by DHCP, reboot the computer 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 (such as WinPoET), you no longer need to run that software after installing your router. If you use Internet Explorer, select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**. Other browsers provide similar options.

Troubleshoot Internet browsing

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet, it might be for the following reasons:

- 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. If your ISP sets a usage limit, they might charge you for the overage. See Unblock the traffic meter after the traffic limit is reached on page 133.
- Your computer 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 router's configuration, restart your computer. Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.
- The router might not be configured as the default gateway on your computer.
  Reboot the computer and verify that the router address (www.routerlogin.net) is listed by your computer 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 (such as WinPoET), you no longer need to

run that software after installing your router. If you use Internet Explorer select **Tools > Internet Options**, click the **Connections** tab, and select the **Never dial a connection**. Other browsers provide similar options.

Changes are not saved

If the router does not save the changes that you make in the router web 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** or **Reload** button in the web browser. It is possible that the changes occurred, but the old settings might be in the web browser's cache.

Troubleshoot WiFi connectivity

If you are experiencing trouble connecting to the router over WiFi, try to isolate the problem:

- Be sure that the WiFi settings in your computer or mobile device and router match exactly. For a computer or mobile device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the router and computer or mobile device must match exactly. The default SSID and password are on the router label.
- Does the computer or mobile device that you are using find your WiFi network? If not, check the WiFi LED on the front of the router. If it is off, you can press the **WiFi On/Off** button on the router to turn the router WiFi radios back on and check to see if the standard LED settings were changed (see Turn the LEDs on or off using the LED On/Off switch on page 18 or Disable or enable LED blinking or turn off LEDs on page 138).
- If you disabled the router's SSID broadcast, then your WiFi network is hidden and does not display in your WiFi client's scanning list (see Specify basic WiFi settings on page 101). By default, SSID broadcast is enabled.
- Does your computer or mobile device support the security that you are using for your WiFi network (WPA or WPA2)?
- If you want to view the WiFi settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, select **System Information**, and locate the Wireless Status pane.

If your computer or mobile device finds your network but the signal strength is weak, check these conditions:

- Is your router too far from your computer or mobile device or too close? Place your computer or mobile device near the router but at least 6 feet (1.8 meters) away and see whether the signal strength improves.
- Are objects between the router and your computer or mobile device blocking the WiFi signal?

Troubleshoot your network using the ping utility

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 or workstation.

Test the path from a Windows-based computer to a remote device

To test the path from a Windows-based computer 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>*
   where *<IP address>* is the IP address of a remote device such as your ISP DNS server.
   If the path is functioning correctly, messages display that are similar to those shown in Test the LAN path to your router on page 208.
3. If you do not receive replies, check the following:
   - Check to see that IP address of your 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 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 cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your computer, enter that host name as the account name on the Internet Setup page.
- 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.

Test the LAN path to your router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the 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 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 occurring:

- Wrong physical connections
  For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.
  Check to see that the appropriate LEDs are lit for your network devices. If your router and computer are connected to a separate Ethernet switch, 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 address for your router and your computer are correct and that the addresses are on the same subnet.

A

Supplemental Information

This appendix includes technical information about your router.

The appendix contains the following sections:

- Factory settings
- Technical specifications

Factory settings

You can return the router to its factory settings. Use the end of a paper clip or a similar object to press and hold the **Reset** button on the back of the router for up to 30 seconds or until the Power LED starts blinking amber. The router resets and returns to the factory configuration settings shown in the following table.

Table 3. Router factory default settings

Feature		Default Setting
Router login	User login URL	www.routerlogin.net or www.routerlogin.com
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	Autosensing
Local network (LAN)	LAN IP address	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	DHCP starting IP address	192.168.1.2
	DHCP ending IP address	192.168.1.254
	DMZ	Disabled
	Time adjusted for daylight saving time	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Table 3. Router factory default settings (Continued)

Feature		Default Setting
General WiFi settings	WiFi communication	Enabled
	Smart Connect	Enabled
	20/40 MHz Coexistence	Enabled
	SSID name	See router label
	Broadcast SSID	Enabled
	Security	WPA2-PSK (AES)
	RF channel	2.4 GHz: Auto 5 GHz for products for world wide use: Channel 44 5 GHz for products for use in North America: Channel 153
	Operating mode	2.4 GHz: Up to 800 Mbps 5 GHz: Up to 1773 Mbps
	CTS/RTS threshold	2347
	Preamble mode	Automatic
	Transmit power control	100%
Guest WiFi network	WiFi communication	Disabled
	Broadcast SSID	Enabled
	SSID name	2.4 GHz band: NETGEAR-Guest 5 GHz band: NETGEAR-5G-Guest
	Security	None (open network)
	Allow guests to see each other and access the local network	Disabled
WPS	WPS capability	Enabled
	Router's WPS PIN	Disabled while Smart Connect is enabled
	Keep Existing Wireless Settings	Disabled

Technical specifications

Table 4. Router technical specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power adapter	North America: 100–240V, 50/60 Hz input UK: 100–240V, 50/60 Hz, input Australia: 220–240V, 50/60 Hz, input Europe: 100–240V, 50/60 Hz input All regions (output): 12V/3.5A DC output
Dimensions	12.7 x 9.6 x 2.2 in. (321.9 x 243.7 x 55.0 mm)
Weight	1.77 lb (801 g)
Operating temperature	0° to 40°C (32° to 104°F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	FCC Part 15 Class B EN 55022 (CISPR 22), Class B C-Tick N10947
LAN	Four RJ-45 ports supporting 10BASE-T, 100BASE-TX, and 1000BASE-T
WAN	One RJ-45 port supporting 10BASE-T, 100BASE-TX, and 1000BASE-T
USB	Two USB 3.0 ports
Wireless	Maximum WiFi signal rate complies with the IEEE 802.11 standard.[1]
Radio data rates	Auto-rate sensing
Data encoding standards	IEEE® 802.11b/g/n 2.4 GHz 256 QAM support IEEE® 802.11a/n/ac 5.0 GHz 256 QAM support[2]
Maximum WiFi clients per WiFi network	Limited by the amount of WiFi network traffic generated by each client (typically 50–70 clients)

Table 4. Router technical specifications (Continued)

Feature	Description
Operating frequency range	2.4 GHz band: • US: 2.412–2.462 GHz • Europe: 2.412–2.472 GHz • Australia: 2.412–2.472 GHz • Japan: 2.412–2.472 GHz 5 GHz band: • US: 5.18–5.24 + 5.745–5.825 GHz and DFS (5.25–5.35 + 5.50–5.70) • Europe: 5.18–5.24 GHz and DFS (5.25–5.35 + 5.50–5.70) • Australia: 5.18–5.24 + 5.745–5.825 GHz and DFS (5.25–5.35 + 5.50–5.70) • Japan: 5.18–5.24 GHz and DFS (5.25–5.35 + 5.50–5.70)
802.11 security	WPA2-PSK, WPA-PSK, WPA/WPA2 (mixed mode), WPA/WPA2 Enterprise, and WEP

[1] *Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.*

[2] *NETGEAR makes no express or implied representations or warranties about this product's compatibility with any future standards.*

Note: For more information, see the data sheet, which is available at downloadcenter.netgear.com.