NETGEAR®

User Manual

Nighthawk Pro Gaming Router

Model XR1000

September 2021
202-12095-02

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

Support and Community

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

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

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

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

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

Trademarks

Contents

Chapter 4 Optimize Gaming and Customize Quality of Service Settings

Chapter 5 Monitor Game Servers and Your Devices, Router, and Network

Chapter 6 Control Access to and From the Internet

Chapter 7 Manage the Router's Network Settings

Chapter 8 Manage the Router's WiFi Settings

Chapter 9 Maintain the Router

Chapter 15 Troubleshooting

Chapter 16 Supplemental Information

1

Hardware Setup

This user manual is for the NETGEAR Nighthawk® Pro Gaming Router XR1000.

The manual describes how you can set up the router and access the router web interface to monitor your network and configure the router features.

This chapter contains the following sections:

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, four antennas, a power adapter, and a flat Ethernet cable. The package also contains the installation guide (not shown in the following figure).

Figure 1. Package contents

LEDs and Buttons on the Top Panel

The status LEDs, **WiFi On/Off** button with LED, and **WPS** button with LED are on the top panel.

Figure 2. Top view

Table 1. LED descriptions

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

Table 1. LED descriptions (Continued)

LED and Button		Description
2.4 GHz	2.4 GHz LED	**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	5 GHz LED	**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.
USB 3.0	USB 3.0 LED	**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.
1 2 3 4	Ethernet ports 1–4 LEDs	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.

Back Panel

The following figure shows the back panel connectors and buttons.

Figure 3. Back panel

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

- **Reset button**. You can press the **Reset** button to reset the router to factory default settings.
  If you press and hold the **Reset** button until the Power LED starts blinking amber, the router restarts and returns to its factory settings. For information about the factory settings, see Factory Settings on page 228.
- **USB 3.0 port**. You can connect a USB storage device to the USB 3.0 port.
- **Ethernet ports**. You can connect a LAN device to each of the four Gigabit Ethernet RJ-45 LAN ports numbered 1 through 4.
- **Internet port**. Connect the yellow Gigabit Ethernet RJ-45 WAN port to a modem such as a cable modem or DSL modem.
- **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.

Note: For information about the antennas, see Attach the Antennas on page 15.

Attach the Antennas

The router comes with four antennas.

- One antenna marked *Ant 1* for antenna post marked *Ant 1* on the right side panel.
- Two antennas marked *Ant 2* for the two antenna posts marked *Ant 2* on the back panel.
- One antenna marked *Ant 3* for the antenna post marked *Ant 3* on the right side panel.

Figure 4. Ant 1 to post 1 and Ant 3 to post 3

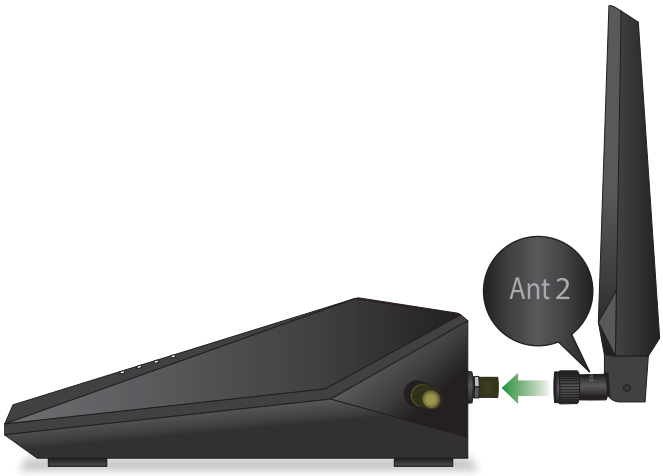


Figure 5. Ant 2 to post 2 (the back panel provides two Ant 2 posts for two Ant 2 antennas)

To attach the antennas:

1. Align the antennas with the antenna posts on the router.

   Observe the markings on the antenna and on the antenna post. Connect each antenna to its corresponding antenna post. The antennas marked *Ant 2* can be attached to either antenna post marked *Ant 2* on the back panel.

2. Attach the antennas on the threaded antenna posts.
3. For the best WiFi performance, place the antennas in a vertical position, as shown in the previous figures.

Router Label

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

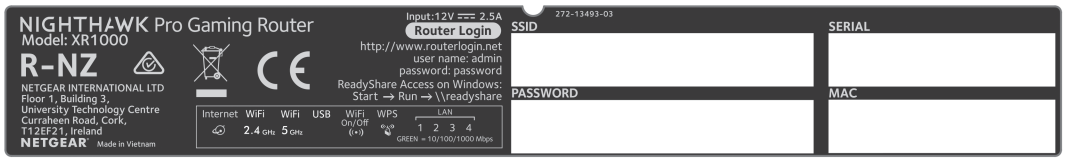


Figure 6. Router label

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.

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
  - Bases of cordless phones
  - 2.4 GHz and 5 GHz cordless phones

- Place the router away from large metal surfaces, large glass surfaces, insulated walls, and items such as these:
  - Solid metal doors
  - Aluminum studs
  - Fish tanks
  - Mirrors
  - Brick
  - Concrete surfaces

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 WiFi routers, WiFi repeaters, WiFi range extenders, and any other device that emits a WiFi signal for network access.

Cable Your Router

Connect your router to a modem and power on your router.

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 connect the power adapter to a power outlet.
4. Press the **Power On/Off** button on the back panel of the router.
   The router's Power LED lights solid white when the router is ready.

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 221. 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 21), 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 Rapps

   For information about these panes, see View Router System Information on page 86.

   For information about how you can change the panes that are shown on the Dashboard, see Customize the Dashboard on page 88.

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 21). 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 27).
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 221.

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 221.

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 32.
   - 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 33.

   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 34
   - Set Up an IPv6 Pass Through Internet Connection on page 36
   - Set Up an IPv6 Fixed Internet Connection on page 36
   - Set Up an IPv6 DHCP Internet Connection on page 37
   - Set Up an IPv6 PPPoE Internet Connection on page 39
   - Set Up an IPv6 6rd Internet Connection on page 41

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. 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. 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. (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. 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 27).
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. 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. 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 29), 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. 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. 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 64 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.
576	Typical value to connect to dial-up ISPs.

4

Optimize Gaming and Customize Quality of Service Settings

You can optimize gaming and customize Quality of Service (QoS) settings to prevent network lag and congestion, to allocate bandwidth to specific devices, and to prioritize traffic for specific devices.

Note: By default, traffic prioritization for automatically classified games is enabled. The classified games are a preset list of games that cover all console games and most PC games. Your router automatically applies traffic prioritization when it detects games.

This chapter contains the following sections:

Decrease lag 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 a range that you can specify. This allows for improved response time and might lead to fairer games.

By default, no devices are added to the Geo Filter and the filter is not in effect. To use the Geo Filter, do the following:

- Add one or more of your local devices to the filter.
- Specify the area in which your devices are located and define the areas in which you play games by *one* of the following methods:
  - **Draw your areas**. Draw the areas in which the servers or hosts that you play on are located and, if applicable, the areas in which other players are located (see Use the Geo Filter by Drawing Areas on page 49).
  - **Set your home area and the distance radius**. Set your home areas and the distance radius, which is the distance to the servers or hosts that you play on and, if applicable, other players (see Use the Geo Filter by Setting Your Home Area and the Distance Radius on page 46).

Note: For information about pinging your favorite game's servers and displaying your connection quality to each server on a world map, see Ping Game Servers and Track Pings Over Time on page 75.

Use the Geo Filter by Setting Your Home Area and the Distance Radius

You can configure the Geo Filter by setting the home area for your devices and the distance radius, which is the distance to the servers or hosts that you play on and to other players.

To configure and use the Geo Filter by setting your home area and the distance radius:

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**.

   The page that displays shows a map.

   For information about the player and server icons that can be shown on the map, see Step 11.

5. To hide the legend for the player and server icons, clear the **Show Legend** check box.
6. To add a device to the Geo Filter, do the following:
   a. Click the **ADD DEVICE** button.
      The Add Device window opens and displays the detected devices.
   b. Select your device.
   c. Click **NEXT**.
   d. Select a game.
      If your device is a console, console games display. If your device is not a console, non-console games displays.
   e. Click **NEXT**.
      If your device is a console, filtering mode is enabled 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, filtering mode is disabled 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 that don't require filtering.
   f. Either override the suggested filter mode or click the **CONTINUE** button.
      Your device is added.
   g. Click the **FINISH** button.
      The Add Device window closes.
7. In the Geo-Filter Map pane, set your home area by clicking the **player** icon and moving the icon onto the map to the country or state in which your devices are located.

   Tip: If the map view is too small, increase the size of the map. You can do so by using your mouse or by moving the vertical slider up in the direction of the + sign. To move the map to the continent in which the best servers are located, click and hold the map and then move it with your mouse.

8. 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.

9. To load the recommended Geo Filter settings for your game, which override your manual distance radius settings, do the following:

   a. In the Geo-Filter Map pane, click the **PROFILES** button.
   The Profile Selector window opens.

   b. Select a game.

   c. Click **DONE**.

10. Allow or block servers, hosts, and players from *outside* your radius by doing the following:

    - **Allow**. Move the **Ping Assist** slider to the maximum ping value in millisecond (ms) that you want to allow for servers, hosts, and players outside your radius. You can also enter the ping value in ms in the field to the right of the slider. For example, if only servers in the UK are allowed by your radius, but a server in Germany tries to connect to you, the Ping Assist option allows that connection if the ping value of the server is below the value that you set for Ping Assist. We recommend you set your Ping Assist value between 30 ms and 50 ms. Any connection with a ping value below the number that you set is allowed to connect to you. You can then increase or decrease the ping value based on your personal preference.
    - **Block**. To disable the Ping Assist option, move the **Ping Assist** slider all the way to the left or enter **0** in the field to the right of the slider. All servers, hosts, and players outside your radius are blocked.

11. 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 blocked devices 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 player and server icons can be shown on the map:

    Player

    Blocked player (a player outside your area or radius)

    Allowed player (a player that you added to the Allowlist)

- Denied player (a player that you added to the Blocklist)
- Ping assist player (a player outside your area or radius that is still allowed)
- Server
- Blocked server (a server outside your area or radius)
- Allowed server (a server that you added to the Allowlist)
- Ping assist server (a server outside your area or radius that is still allowed)

Note: For information about allowing or blocking a connection to a device (to a player or server), see Ping a Device and Allow or Deny the Device a Connection on page 53.

If the Auto Ping Host option is enabled, a ping graph automatically displays when you are in a game (see View the Automatically Generated Ping Graph for a Connection on page 54). Otherwise, you can manually click any icon on the map to load a ping graph for that connection.

12. 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 Options pane displays.
    b. Select the **Auto Ping Host** check box.
    c. Click the **X**.
    The Settings pane closes.

Use the Geo Filter by Drawing Areas

You can configure the Geo Filter by drawing the home area for your devices, one or more areas for the servers or hosts that you play on, and, if applicable, one or more areas for other players. For example, if you determine the best server to play on, you can draw an area around that server. All connections from outside the areas that you draw are blocked.

We refer to the drawing option as Polygon Mode and we refer to the action of drawing areas as Geo Fencing.

To configure and use the Geo Filter by drawing your areas:

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**.

   The page that displays shows a map.

   For information about the player and server icons that can be shown on the map, see Step 9.

5. To hide the legend for the player and server icons, clear the **Show Legend** check box.
6. To add a device to the Geo Filter, do the following:
   a. Click the **ADD DEVICE** button.
      The Add Device window opens and displays the detected devices.
   b. Select your device.
   c. Click **NEXT**.
   d. Select a game.
      If your device is a console, console games display. If your device is not a console, non-console games displays.
   e. Click **NEXT**.
      If your device is a console, filtering mode is enabled 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, filtering mode is disabled 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 that don't require filtering.
   f. Either override the suggested filter mode or click the **CONTINUE** button.
      Your device is added.
   g. Click the **FINISH** button.
      The Add Device window closes.
7. In the Geo-Filter Map pane, draw your home area in which your devices are located, draw one or more areas for the servers or hosts that you play on, and draw one or more areas for other players by doing the following:

Tip: If the map view is too small, increase the size of the map. You can do so by using your mouse or by moving the vertical slider up in the direction of the + sign. To move the map to the continent in which the best servers are located, click and hold the map and then move it with your mouse.

a. Click the **Polygon Mode** button.
The button displays red and Polygon Mode is enabled.

b. Click the **pencil** icon.
Drawing Mode is enabled.

c. Draw your home area: Click the first point on the map, draw a line to a second point, click again, draw a line to a third point, click again, and so on until you connect the last line to your first point.
Other than a circle and an oval, you can draw any shape: a triangle, square, rectangle, pentagon, and so on.

d. Draw one or more areas for the servers or host and other players: Click the first point on the map, draw a line to a second point, click again, draw a line to a third point, click again, and so on until you connect the last line to your first point.
You can draw multiple areas in multiple shapes. You can set a maximum number of 50 points on the map, but these points do not need to be connected. For example, you could set up 3 areas, each consisting of 6 points, which counts as 18 points.

e. When you are finished drawing, exit Drawing Mode by clicking the **X**.

Note: To remove an area that you drew so you can redefine it, click the **trashcan** icon to enable Deletion Mode, and then click the area on the map. To disable Deletion Mode, click the **trashcan** icon again.

All connections from outside the areas that you drew are blocked.

8. To allow or block servers, hosts, and players from *outside* the areas that you drew:

- **Allow**. Move the **Ping Assist** slider to the maximum ping value in millisecond (ms) that you want to allow for servers, hosts, and players outside your radius. You can also enter the ping value in ms in the field to the right of the slider.
For example, if only servers in the UK are allowed by the areas that you drew, but a server in Germany tries to connect to you, the Ping Assist option allows that connection if the ping value of the server is below the value that you set for Ping Assist.
We recommend you set your Ping Assist value between 30 ms and 50 ms. Any connection with a ping value below the number that you set is allowed to connect to you. You can then increase or decrease the ping value based on your personal preference.

- **Block**. To disable the Ping Assist option, move the **Ping Assist** slider all the way to the left or enter **0** in the field to the right of the slider. All servers, hosts, and players outside your radius are blocked.

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 blocked devices 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 (a player outside your area or radius)

    Allowed player (a player that you added to the Allowlist)

    Denied player (a player that you added to the Blocklist)

    Ping assist player (a player outside your area or radius that is still allowed)

    Server

    Blocked server (a server outside your area or radius)

    Allowed server (a server that you added to the Allowlist)

    Ping assist server (a server outside your area or radius that is still allowed)

   Note: For information about allowing or blocking a connection to a device (to a player or server), see Ping a Device and Allow or Deny the Device a Connection on page 53.

   If the Auto Ping Host option is enabled, a ping graph automatically displays when you are in a game (see View the Automatically Generated Ping Graph for a Connection on page 54). 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 Options 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 or defined areas of your Geo Filter. If you allow an individual connection, the device can connect to your device, even if is outside the radius or defined areas of your Geo Filter. If you deny an individual connection, the device cannot connect to your device, even if is inside the radius or defined areas of your Geo Filter. However, you cannot block a dedicated server.

To ping a device and allow or deny a connection 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**.
   The page that displays shows a map.
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 show 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:
   - **50 ms or lower**. Very good for online gaming.
   - **50 ms–100 ms**. Good for online gaming.
   - **100 ms–150 ms**. Acceptable for online gaming.
   - **150 ms or higher**. Unfavorable for online gaming.
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 **trashcan** icon in the Allow and Deny pane.
   If the connection was allowed, it might now be denied if it is outside the distance radius or your defined areas.

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

View the Automatically Generated Ping Graph for a Connection

By default, the Auto Ping Host option is enabled. That means that for a connection between your device and another device, a ping graph is automatically generated, showing the connection quality. For more information about the Auto Ping Host option, see Manage the Geo Filter Map Settings on page 57.

To view the automatically generated ping graph for a 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 **Geo-Filter**.
   The page that displays shows a map.

   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.

   In the Auto Ping pane, the following information displays for the connection:

   - **Ping**. 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:
     - **50 ms or lower**. Very good for online gaming.

  - **50 ms–100 ms**. Good for online gaming.
  - **100 ms–150 ms**. Acceptable for online gaming.
  - **150 ms or higher**. Unfavorable for online gaming.

- **Host Tick Rate**. The number of packets sent per second from the host of your game (usually a server) to you. The higher the tick rate, the better.
- **Client Tick Rate**. The number of packets per second that your device is sending to the host of your game.
- **Send Rate**. The amount of data per second that the host of your game sends to your device.
- **Receive Rate**. The amount of data per second that your device is sending to the host of your game.

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**.
   The page that displays shows a map.
5. Click the **ADD DEVICE** button.
   The Add Device window opens and displays the detected devices.
6. Select your device.
7. Click **NEXT**.
8. Select a game.
   If your device is a console, console services display. If your device is not a console, nonconsole services displays.

9. Click **NEXT**

   If your device is a console, filtering mode is enabled 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, filtering mode is disabled 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 that don't require filtering.

10. Either override the suggested filter mode or click the **CONTINUE** button.
    Your device is added.

11. Click the **FINISH** button.
    The Add Device window closes.

    Note: For information about using the device with the Geo Filter, see Use the Geo Filter by Setting Your Home Area and the Distance Radius on page 46 or Use the Geo Filter by Drawing Areas on page 49.

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**.
   The page that displays shows a map.
5. Move your mouse over the device that you want to remove.
6. When the **DELETE** button displays below the device, click the **DELETE** button.
   The device is removed from the Geo Filter.

Manage the Geo Filter Map Settings

You can manage the 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, whether the Auto Ping Host feature is enabled, and whether the Fast Search feature is enabled.

Fore information about using the Geo Filter, see Use the Geo Filter by Setting Your Home Area and the Distance Radius on page 46 or Use the Geo Filter by Drawing Areas on page 49.

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**.
   The page that displays shows a map.
5. In the Geo-Filter Map pane, click the **Geo-Filter Map menu** icon.
   The Options pane displays.
6. Configure the following 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 53).

- **Fast Search**. The Fast Search feature enabeld the Ping Assist feature to work faster, which, in turn, lets you find games quicker. By default, the **Fast Search** check box is selected. However, with Fast Search enabled, occasionally a connection might be allowed for a device with a ping value that is higher than the value that you set for the Ping Assist feature. If you do not want that to happen, clear the **Fast Search** check box.

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 Options pane, click the **X**.

Run and Manage Connection Benchmark Tests

Before you enable congestion control, we recommend that you run at least one connection benchmark test to determine your Internet upload and download speed for traffic and pings.

You can then use the test results to configure congestion control (see Prevent Network Congestion With Congestion Control on page 61).

Run a Connection Benchmark Test

You can run a connection benchmark test and save the test results in the test history.

To run a connection benchmark test:

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 **Connection Benchmark**.
5. On the Connection Test page, click the **RUN TEST** button.

The router runs the following tests:

- **Speed Test**. The traffic upload and download speed in Mbps.
- **Ping Test**. The ping speed and jitter in ms as well as any packet loss as a percentage.
- **Ping Test (Under Load)**. The ping upload, download, and idle time speed in ms (also referred to as bufferbloat).

The test results are graded, for example, A+, A, or B, and saved in the Test History pane so that you can review the tests again later.

Schedule Connection Benchmark Tests

You can schedule a one-time test or recurring tests.

To schedule connection benchmark tests:

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 **Connection Benchmark**.
5. In the lower right of the page, click **Scheduled Tests**.
   The Scheduled Tests pane displays.
6. Click the **SCHEDULE TEST** button.
   The Add Scheduled Test window opens.
7. Either add a one-time test or a recurring test:
   - **One-time test**. Do the following:
     a. From the upper menu, select **One Time**.
     b. From the lower menus, select the hour, minutes, date, and month.
     c. Either leave the **Allow Test While Internet Is In Use** check box or clear it.
     d. Click the **ADD** button.
        The test is scheduled.

- **Recurring test**. Do the following:
  a. From the upper menu, select **Repeating**.
  b. From the lower menu, select the frequency from 1 to 24 hours.
  You can also select **Custom** and specify a custom schedule.
  c. Either leave the **Allow Test While Internet Is In Use** check box or clear it.
  d. Click the **ADD** button.
  The tests are scheduled.

Manage if Tests Can Be Scheduled or Delete Tests

You can manage if tests can be scheduled at all, delete scheduled tests, delete failed tests, or delete all tests.

To manage if tests can be scheduled or delete tests:

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 **Connection Benchmark**.
5. To delete a scheduled test, do the following:
   a. In the lower right of the page, click **Scheduled Tests**.
   The Scheduled Tests pane displays.
   b. Click the **trashcan** icon for the scheduled test.
   A confirmation window displays.
   c. Click the **Confirm** button.
   The scheduled test is deleted.

6. To manage the scheduling of tests, delete failed tests, or delete all test, do the following:
   a. Click the **Connection Test menu** icon.
      The the Options pane displays.
   b. Do one of the following:
      - **Enable Scheduled Tests**. By default, the scheduling of tests is enabled and the button displays red. To disable the scheduling of tests, click the button. If scheduling is disabled, the button displays white.
      - **Delete failed tests**. Click the **DELETE FAILED TESTS** button.
      - **Delete all tests**. Click the **DELETE ALL TESTS** button.
   c. To close the Options pane, click the **X**.

Manage Bandwidth Allocation

The router supports a Quality of Service (QoS) feature that lets you prevent network congestion by controlling the total bandwidth and allocating bandwidth to either specific types of applications or specific devices.

Prevent Network Congestion With Congestion Control

If you enable congestion control, the router can prevent network congestion and queuing delays caused by applications or devices that consume a lot of bandwidth. You can set the maximum percentage of the total bandwidth that bandwidth-intensive applications or devices can consume. This allows bandwidth to remain available for applications or devices that consume less bandwidth.

To enable and configure congestion control:

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 Congestion Control pane, click the **Congestion Control menu** icon.
   The Options pane displays.
6. In the **Download Bandwidth** and **Upload Bandwidth** fields, enter your Internet download bandwidth speed in Mbps and Internet upload bandwidth speed in Mbps.
   If you used the automatic Internet setup (see Automatic Internet Setup on page 21), the bandwidth speeds were automatically entered. If you are not sure about your Internet bandwidth speeds, or you would like to redefine the bandwidth speeds, run a connection benchmark test (see Run a Connection Benchmark Test on page 58).
7. Set the default congestion control 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 QoS**. By default, the **Disable QoS** check box is cleared. If you disable all QoS features, the router can no longer prevent network congestion and other features, such a Deep Packet Inspection, are also disabled. We recommend that you do not select this check box but keep QoS enabled.
8. Click the **X** to close the Options pane.
9. Select how you want to apply congestion control:
   - **Always**. Select this radio button to always apply congestion control. With this setting, you can play games without any applications or devices causing traffic to lag, but your total bandwidth speed is reduced. We recommend that when you finish gaming, you set the setting back to **Never**.
   - **Auto-Enable**. Select this radio button to let the router automatically apply congestion *only* if games are being played (all console games and most computer games are automatically detected). Your total bandwidth speeds are reduced only if games are detected.
   - **Never**. Select this radio button to disable congestion control. With this setting, your full bandwidth speeds are available, but if all your bandwidth is being used, your games are subject to a queue, causing traffic to lag. This radio button is selected by default.
10. In the Congestion Control 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, applications or 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 applications or devices that consume less bandwidth.

Tip: For gaming, we recommend that you set each slider to 70 percent.

Disable Congestion Control

If you disable congestion control, bandwidth-intensive applications and devices can consume all available bandwidth, causing congestion and forcing traffic for other applications and devices to be queued. However, situations might exist in which you want to disable congestion, even if it is temporarily.

To disable congestion control:

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 Congestion Control pane, move the buttons on the **Download** and **Upload** sliders all the way to the right, to 100 percent.
   Congestion control is now disabled.

Allocate Bandwidth to Devices

Note: You can allocate bandwidth either to types of applications or to devices. These bandwidth allocation modes are mutually exclusive.

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**.
5. In the Bandwidth Allocation pane, click the **Bandwidth Allocation menu** icon.
   The Options pane opens.
6. Select the **Devices** radio button and click the **X** to close the Options pane.
   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.
7. 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 that device.

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

8. 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 that device.

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

9. 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**.

10. 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 Options pane opens.
    b. Clear the **Download Share Excess** check box.
    The download bandwidth that you allocate to each device is now the maximum download bandwidth that the device can use. Any excess download bandwidth is not shared.
    c. Clear the **Upload Share Excess** check box.
    The upload bandwidth that you allocate to each device is now the maximum upload bandwidth that the device can use. Any excess upload bandwidth is not shared.
    d. To close the Options pane, click the **X**.

Allocate Bandwidth to Types of Applications

Note: You can allocate bandwidth either to types of applications or to devices. These bandwidth allocation modes are mutually exclusive.

Some types of applications on your network need more bandwidth than others. For example, applications that you use for gaming or media streaming require more bandwidth than applications that are mostly used for browsing or messaging and chatting. You can allocate a percentage of the total router bandwidth to each type of application on your network. Doing so guarantees bandwidth for an application when it needs it.

You can set different allocations for upload and download bandwidths.

By default, the router automatically allocates excess (unused) bandwidth to an application 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 type of application is the maximum bandwidth that the type of application can use.

To allocate bandwidth to types of applications:

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 Bandwidth Allocation pane, click the **Bandwidth Allocation menu** icon.

   The Options pane opens.

6. Select the **Applications** radio button and click the **X** to close the Options pane.

   The Bandwidth Allocation pane displays a graph that shows the types of applications on the router network. By default, each type of application is allocated an equal share of the router bandwidth, expressed by a number in a white circle that is associated with the type of application.

7. To allocate download bandwidth to types of applications, 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 type of application 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 types of applications change.

      CAUTION: If you allocate 100 percent to one type of application, you effectively disable other types of applications. If you allocate 0 percent to one type of application, you effectively disable that type of application.

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

8. To allocate upload bandwidth to types of applications, 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 type of application 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 types of applications change.

CAUTION: If you allocate 100 percent to one type of application, you effectively disable other types of applications. If you allocate 0 percent to one type of application, you effectively disable that type of application.

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

9. To allocate an exact bandwidth (either in Mbps or in percentage) to a type of application, 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 with types of applications to the left of the graph, select the type of application.
   If no types of applications 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 type of application also affects available bandwidth for other types of applications.
   e. To close the pane, click the **X**.

10. 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 Options pane opens.
    b. Clear the **Download Share Excess** check box.
    The download bandwidth that you allocate to each type of application is now the maximum download bandwidth that the type of application can use. Any excess download bandwidth is not shared.
    c. Clear the **Upload Share Excess** check box.

The upload bandwidth that you allocate to each type of application is now the maximum upload bandwidth that the type of application can use. Any excess upload bandwidth is not shared.

d. To close the Options pane, click the **X**.

Reset the Bandwidth Distribution

You can reset the bandwidth to default settings so that the router allocates each type of application or 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 Service 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 73).

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 service 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 automatically classified games is enabled. The classified games are a preset list of games that cover all console games and most PC games. If you enable traffic prioritization for all classified games, your router automatically applies traffic prioritization when it detects games. We recommend that you keep this setting enabled.

   You can manually add a service, port, or port range by clicking the **ADD DEVICE** button and then choosing a service, port, or port range to add. However, if the service, port, or port range that you add is used for high-bandwidth intensity applications, traffic congestion might occur.

6. To manually add a device and service, port, or port range for traffic prioritization, do the following in the Traffic Prioritization pane:
   a. Click the **ADD DEVICE** button.
      The Traffic Prioritization Selector window opens and the detected devices display.
   b. Select your device.
   c. Click **NEXT**.
   d. Select a service.
      By default, the **Basic** radio button is selected and a preset list of services and games display. We recommend that you manually select a service only if you consider yourself an advanced user.
      Instead of selecting a service, you can also manually add a port or port range and a protocol. See the next step.
   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.

For each device (target) and service, the Traffic Prioritization Information pane displays the total number of downloaded packets and the total number of uploaded packets. If high-priority traffic is automatically being prioritized, a colored circle displays in the Download Packets and Upload Packets columns.

The Traffic Overview pane displays the total number of prioritized downloaded packets, the total number of prioritized uploaded packets, the total number of downloaded background packets, and the total number of uploaded background packets

Add a Device and a Service for Traffic Prioritization

You can manually add a device for which you then can choose a service for traffic prioritization. If you consider yourself an advanced user, you can add a port or port range for traffic prioritization.

If the service, port, or port range that you add is used for high-bandwidth intensity applications, traffic congestion might occur.

To add a device and a service, port, or port range 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. Click the **ADD DEVICE** button.

   The Traffic Prioritization Selector window opens and the detected devices display.

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

   By default, the **Basic** radio button is selected and a preset list of games display.

   Instead of selecting a service, you can manually add a port or port range and a protocol. See the next step. We recommend that you do this only if you consider yourself an advanced user.

10. To display advanced 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, traffic for services that you manually added for 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**.

   In the Traffic Prioritization pane, to the left of All Devices, the button displays as a red circle because automatic traffic prioritization is enabled.
5. Click the button so that it displays as a white circle.

   High-priority traffic is no longer automatically prioritized.

5

Monitor Game Servers and Your Devices, Router, and Network

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

For information about viewing the router logs, network statistics, and network connections, see Maintain the Router on page 148.

The chapter includes the following sections:

Ping Game Servers and Track Pings Over Time

You can ping the servers for your favorite games to determine the best servers to connect to and the ones to avoid. For each server for a specific game, your connection quality displays on a world map. You can also build a ping history for your favorite servers so that you can monitor the quality of the servers you play on over time.

This information can help you to define your Geo Filter settings so that you can play on the best (lag-free) servers and block servers with poor connections. For more information, see Decrease lag by Using the Geo Filter on page 46.

Ping Game Servers for a Specific Game

You can ping the game servers for a specific game to determine the best servers to connect to for that game. You can also schedule a ping to occur on a regular basis for a selected server, enabling the router to establish a ping history for the server and allowing you to track pings over time.

You can assemble your own custom lists of servers so that the router can ping them as a group, separately from the game based lists they came from. You can also track a server separately from other game servers.

To ping game servers for a specific game and add a server to a custom ping 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 **Ping Heatmap**.
   The page that displays shows a map.
5. From the **Select Ping Target** menu, select a game.
   If your game is not listed, you can add a custom ping list (see Add a Custom Ping List on page 78).
   The detected servers display on the map, with the ping time in ms listed above each server. Green indicates servers with the best connection time, yellow with a moderate

connection time, and red with the worst connection time. A collection of servers might display as a cluster, which you can expand by clicking on the cluster.

Tip: If the map view is too small, increase the size of the map. You can do so by using your mouse or by moving the vertical slider up in the direction of the + sign. To move the map to the continent in which the best servers are located, click and hold the map and then move it with your mouse.

If you schedule ping tracking (see Step 9), you can select a time span from the **Slider Timespan** menu to the right below the map and move the slider below the map to view a specific period within the selected time span. Doing so lets you compare the pings to the servers for the game over time.

6. To manually ping the servers again for the same game, click the **PING AGAIN** button.
   The information on the map is updated. By default, manual pings are saved in the ping history.

7. To view information about one server and open the ping history pane for that server, do one of the following.

   - **Use the map**. On the map, click the server.
     At the bottom of the page, the ping history pane opens, displaying information about the server.
   - **Use the menu**. Do the following:
     a. To the right of the colored bar above the map, click the **menu** icon.
        A pane with the IP addresses displays. These are the IP addresses of all servers that were pinged for the specific game.
     b. Click the IP address of the server.
        At the bottom of the page, the ping history pane opens, displaying information about the server.
     c. To close the pane with IP addresses, click the **>** button.

   The ping history pane shows the current ping time for the server. If you pinged the server before, the pane shows the average ping time, indicated by the dotted line, and the current ping time, indicated by a white arrow at the right.

   You can select a time span from the **Slider Timespan** menu to the right below the map and move the slider below the map to view a specific period within the selected time span. Doing so lets you compare the pings to the specific server over time.

8. To add the server on the ping history pane to an existing or new custom ping list, do one of the following:

   - **Add the server to an existing custom ping list**. Do the following:
     a. Click the **ADD TO LIST** button.
        The Add to Lists window opens and shows the list names that you already added (see Add a Custom Ping List on page 78).
     b. Select the check box for a list.
     c. Click the **SAVE** button.
        The server is added to the existing list.

   - **Add the server to a new custom ping list**. Do the following:
     a. Click the **ADD TO LIST** button.
        The Add to Lists window opens.
     b. Click the **ADD NEW LIST** button
        The Custom List window opens.
     c. Type a name for the list.
        The name helps you to identify the list.

        Note: Because you are adding the IP address of the server, the **ADD IP ADDRESS** button is not relevant in this task. For more information about this button, see Add a Custom Ping List on page 78.

     d. To allow the router to schedule pings, click the **clock** icon. In the Tracking window that displays, from the menu at the top, select how often the router must ping the server. Then, select the days on which the router must ping the server. Finally, click the **DONE** button.
     e. Click the **SAVELIST** button.
        The Add to Lists window displays again.
     f. Select the check box for the list that you just added.
     g. Click the **SAVE** button.
        The server is added to your new list.

9. To schedule pings for the servers for the same game so you can track the pings over time, do the following:
   a. Above the map, click the **clock** icon.
      The Tracking window opens.
   b. From the menu at the top, select how often the router must ping the servers.

c. Select the days on which the router must ping the servers.

d. Click the **SAVE** button.
The pings are scheduled. Next to the clock icon, the time of the next scheduled ping is shown.
For information about viewing the ping history, see View the Ping History for One or More Servers for a Specific Game on page 80.

Add a Custom Ping List

If your game is not listed in the predefined list of games that you can ping (see Ping Game Servers for a Specific Game on page 75), you can add one or more IP addresses for servers that support your game. To set up the list, you must know the IP addresses.

To add a custom ping list with IP addresses:

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 **Ping Heatmap**.
   The page that displays shows a world map.
5. Click the **Ping Heatmap menu** icon.
   The Options pane displays.
6. Click the **ADD CUSTOM LIST** button.
   The Custom List window opens.
7. Type a name for the list.
   The name helps you to identify the list.
8. To allow the router to schedule pings for the IP addresses on your list, do the following:
   a. Click the **clock** icon.
      The Tracking window displays.
   b. From the menu at the top, select how often the router must ping the servers.

c. Select the days on which the router must ping the servers.

d. Click the **DONE** button.
The pings are scheduled.

9. Click the **ADD IP ADDRESS** button.
The window adjusts.

10. Add one or more IP addresses by using one of the following methods:

- **Add a single IP address**. Type a name for the server, enter the IP address in the fields below the name, click the **+** button, and then click the **SAVELIST** button.
- **Add several IP addresses**. Type a name for the server, enter the IP address in the fields below the name, click the **+** button, and repeat the process for another IP address. After you add all your IP addresses to the list, click the **SAVELIST** button.
- **Add multiple IP addresses**. Click the **BULK ADD** button, enter an IP address followed by a space and the server name (for example, 127.0.0.1 local), press **Enter**, and repeat the process for each IP address and name that you want to add. After you add all your IP addresses to the list, click the **SAVE** button and then click the **SAVELIST** button.

Your custom list is added to the menu in the list of games that you can ping.

Change a Custom Ping List

You can change any setting for a custom ping list.

To change a custom ping 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 **Ping Heatmap**.
The page that displays shows a world map.

5. In the **Select Ping Target** menu, click the **pencil** icon for the list that you want to change.
   The Custom List window opens.
6. Change the settings for the ping list. For more information about the settings, see Add a Custom Ping List on page 78.
7. After you changed the settings, click the **SAVELIST** button.
   Your settings are saved.

Delete a Custom Ping List

You can delete a custom ping list that you no longer need.

To delete a custom ping 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 **Ping Heatmap**.
   The page that displays shows a world map.
5. In the **Select Ping Target** menu, click the **pencil** icon for the list that you want to change.
   The Custom List window opens.
6. Click the **DELETE LIST** button.
   The list is removed.

View the Ping History for One or More Servers for a Specific Game

If you scheduled ping tracking for the servers for a specific game (see Ping Game Servers for a Specific Game on page 75) or you added a custom ping list and added ping tracking for the server or servers on the custom ping list, you can view the ping history for a server.

To view the ping history for a 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 **Ping Heatmap**.
5. From the **Select Ping Target** menu, select a game or a custom ping list that you added before.
   The detected server or servers display on the map.

   Tip: If the map view is too small, increase the size of the map. You can do so by using your mouse or by moving the vertical slider up in the direction of the + sign. To move the map to the continent in which the best servers are located, click and hold the map and then move it with your mouse.

   If you schedule ping tracking (see Ping Game Servers for a Specific Game on page 75), you can select a time span from the **Slider Timespan** menu to the right below the map and move the slider below the map to view a specific period within the selected time span. Doing so lets you compare the pings to the servers for the game over time.
6. To open the ping history pane for a server, do one of the following.
   - **Use the map**. On the map, click the server.
     At the bottom of the page, the ping history pane opens, displaying information about the server.
   - **Use the menu**. Do the following:
     a. To the right of the colored bar above the map, click the **menu** icon.
        A pane with the IP addresses displays. These are the IP addresses of all servers that were pinged for the specific game.
     b. Click the IP address of the server.
        At the bottom of the page, the ping history pane opens, displaying information about the server.
     c. To close the pane with IP addresses, click the **>** button.

The ping history pane shows the current and historical ping times for the server. The pane shows the average ping time, indicated by the dotted line, and the current ping time, indicated by a white arrow at the right.

You can select a time span from the **Slider Timespan** menu to the right below the ping history pane and move the slider below the pane to view a specific period within the selected time span. Doing so lets you compare the pings to the specific server over time.

Manage the Ping Heatmap Settings

You can manage the Ping Heatmap settings such as whether detected server clusters are expanded on the map and whether manual pings are saved.

Fore information about pinging game servers, see Ping Game Servers for a Specific Game on page 75.

To manage the Ping Heatmap 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 **Ping Heatmap**.
   The page that displays shows a world map.
5. Click the **Ping Heatmap menu** icon.
   The Options pane displays.
6. Configure the following general settings:
   - **Ping Cluster Default**. By default, clusters of servers are expanded on the map so that individual servers are displayed. To disable this option so that clusters are displayed on the map, click the **Ping Cluster Default** button so that the button displays as a white circle.
   - **Save Manual Pings**. By default, the router saves manual pings that you add through clicking the **PING AGAIN** button on the Ping Heatmap page. To disable this option so that manual pings are not saved, click the **Save Manual Pings** button so that the button displays as a white circle.

Note: For information about adding a custom ping list, see Add a Custom Ping List on page 78.

7. To sync the server information in the cloud with the information on your device, click the **FORCE CLOUD UPDATE** button.

   In most situations, the sync process occurs automatically. However, a situation might occur in which you want to force the cloud update.

8. To close the Options pane, click the **X**.

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 Optimize Gaming and Customize Quality of Service Settings on page 45).

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 **Upload**.
     The Upload text is crossed out and the graph displays the download bandwidth only. Click **Upload** again to redisplay the upload bandwidth.
   - To exclude download bandwidth from the pane, above the graph in a pane, click **Download**.
     The Download text is crossed out and the graph displays the upload bandwidth only. Click **Download** 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 by default:
   - **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 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 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 amount of traffic that was transferred since your started the router. The information includes the transmitted and received bytes, packets, and unprioritized packets (packets that did not reach their destination).
- **Installed Rapps**. This pane shows the default router applications (Rapps) that are installed on the router.

  Note: 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 Internet connection type, WAN IP address, and Internet connection status of the router.

- **Wireless Status**. The information in this pane includes the network name (SSID), network key (WiFi password), and type of WiFi security for the 2.4 GHz radio and 5 GHz radio in the main WiFi network.
- **Guest Wireless Status**. This information in this pane includes the network name (SSID), network key (WiFi password), and type of WiFi security 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
- Guest Wireless Status
- Wireless Status
- Network Overview
- CPU Usage
- Installed Rapps

For information about these panes except for the Network Overview pane, see View Router System Information on page 86. For information about the Network Overview pane, see View Network Usage Information on page 84.

You can customize the panes that display on the Dashboard by adding panes that are useful to you and removing panes that are not. You can 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 a pane to the Dashboard, do the following:
   a. Select one of the following from the router menu on the left of the page: **Geo-Filter**, **Ping Heatmap**, **QoS**, **Connection Benchmark**, **Device Manager**, **Network Monitor**, **Traffic Controller**, or **System Information**.
      The page displays panes.
   b. Click the **pin** icon that is associated with the pane that you want to add to the Dashboard
      The pane is added to the Dashboard.
   c. To add another pane to the Dashboard, repeat the previous two steps.

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 the title banner of 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 and From the Internet

The router comes with a built-in firewall that helps protect your network from unwanted intrusions from the Internet. You can also set up traffic rules to allow, block, or reject all traffic, particular categories of traffic, specific games, or port ranges.

This chapter includes the following sections:

Manage NETGEAR Armor

Your router supports NETGEAR Armor.

After you start your subscription, NETGEAR Armor protects your home network from potential cyber threats and provides complete data protection, advanced threat defense, webcam protection, multilayer ransomware protection, anti-phishing, safe files, secure browsing, rescue mode, anti-fraud, and anti-theft. In addition, NETGEAR Armor provides multiple performance and privacy tools.

NETGEAR Armor can support features for your Windows-based computers and your Mac OS, iOS, and Android devices.

For more information about NETGEAR Armor, visit netgear.com/landings/armor/default.aspx.

You can manage NETGEAR Armor from the Nighthawk app. You can also view or change your Armor settings from the NETGEAR Armor portal.

Activate Armor Using the Nighthawk App

To activate Armor using the Nighthawk app:

1. Launch the Nighthawk app.
   The dashboard displays.
2. Tap **Security**.
   The Armor page displays.
3. Tap the **ACTIVATE** button.
   Armor is activated.

View or Change Your NETGEAR Armor Settings Using the Nighthawk App

To view or change your NETGEAR Armor settings using the Nighthawk app:

1. Launch the Nighthawk app.
   The dashboard displays.
2. Tap **Security**.
   The Armor page displays.

   You can now view or change the settings.

View or Change your NETGEAR Armor Settings From the Armor Portal

If you already activated NETGEAR Armor, you can view or change your NETGEAR Armor settings from the NETGEAR Armor portal.

To view or change your NETGEAR Armor settings:

1. Launch a web browser and visit armor.netgear.com.
   The NETGEAR account sign in page displays.
2. Enter your NETGEAR account email address and password in the fields and then click the **Sign In** button.
   The NETGEAR Armor portal displays.

Allow, Block, or Reject Traffic Categories, Specific Games, or Port Ranges With Traffic Rules

You can set up traffic rules to allow, block, or reject all traffic, particular categories of traffic, specific games, or port ranges. You can apply a traffic rule to one or more specific devices or to all devices on your network, and you can set up a schedule for each traffic rule. You can also apply a traffic rule to all devices and then set up an exception for a device.

For each traffic rule, you can set up *one* of the following filtering actions:

- **Block**. This action blocks traffic that conforms to the rule but allows all other traffic. When traffic is blocked, it is dropped *without* notification to the traffic source.
- **Allow**. This action allows traffic that conforms to the rule but blocks all other traffic.
- **Reject**. This action rejects traffic that conforms to the rule but allows all other traffic. When traffic is rejected, it is dropped *with* a notification to the traffic source. This action is available only for a rule that applies to all traffic or to a port range. It is not available for a rule that applies to particular categories of traffic or to specific games.

As you add rules, they are added to the table of rules, with the rule at the top of the table as the most important rule that takes priority over all other rules. The second rule in the table takes priority over all other rules that follow in the table, and so on. The rule at the bottom of the table is the least important rule that is applied only after all other rules were applied. However, you can reorder the rules in the table.

As an example, if you want to block every port except for one on your smart home device, set up a first rule that allows traffic on that port on your smart home device. Then, set up a second rule that blocks all traffic on your smart home device.

Add a Rule to Allow, Block, or Reject Traffic

Before you add a traffic rule, consider the following:

- **Devices**. Which devices will the rule apply to? The rule can apply to all devices or to one or more specific devices.
- **Traffic**. Which traffic will the rule apply to? The rule can apply to all traffic, one or more particular categories of traffic, one or more specific games, or a port range.
- **Action**. What will be the action of the rule? The rule can allow, block, or, for all traffic or a port range, reject traffic.
- **Duration**. When will the rule be in effect? The rule can be in effect continuously or on specific days and at specific times.
- **Priority**. What will be the priority of the rule in relation to other rules. For information about reordering your rules, see Reorder the Priority of a Traffic Rule on page 96.

To add a rule to allow, block, or reject traffic:

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 **Traffic Controller**.
5. In the Traffic Rules pane, click the **ADD RULE** button.
   The Add Rule window opens.
6. Type a name for your rule.
   The name helps you to identify the rule.
7. To allow the router to track events for the rule (for example, when a rule is applied to traffic), leave the **Event Capture** check box selected (it is by default).
   To disable even tracking for the rule, clear the **Event Capture** check box.

8. Click **NEXT**.
9. Either select the **All Devices** check box or select one or more devices from the list of detected devices.
10. Click **NEXT**.
11. From the **Select Target** menu, select the type of traffic to which the rule must apply:
    - **All Traffic**. The rule applies to all traffic.
    - **Port Range**. Specify the source start and end ports, the destination start and end ports, and the protocol or protocols.
    - **Application**. Select one or more games.
    - **Category**. Select one or more traffic categories.
12. Click **NEXT**.
13. From the **Allow or Block Traffic** menu, select one of the following actions for the rule:
    - **Allow**. Allows traffic that conforms to the rule but blocks all other traffic.
    - **Block**. Blocks traffic that conforms to the rule but allows all other traffic. When traffic is blocked, it is dropped *without* notification to the traffic source.

      CAUTION: Make sure that your first traffic rule does not block all traffic for all devices because your connection to the router web interface might be terminated and you might need to reset the router to factory default settings to regain access.

    - **Reject**. Rejects traffic that conforms to the rule but allows all other traffic. When traffic is rejected, it is dropped *with* a notification to the traffic source. This action is available only for a rule that applies to all traffic or to a port range. It is not available for a rule that applies to particular categories of traffic or to specific games.

    By default, the rule applies continuously.
14. To specify that the rule must apply to specific days and times, do the following:
    a. **Days**. Select or clear the check boxes for individual days on which the rule must be active.
    b. **Times**. In the AM circle, PM circle, or both, click the hours that the rule must be active.
       If you click a hour segment (for example, the 9-to-10 segment), the color changes. To reset the times, click the **Toggle All** button under the AM circle or PM circle.
15. Click **DONE**.

The rule is added to the Traffic Rules table.

Traffic information about the rule displays in the Traffic Analysis pane. If you enabled event capture, events for the rule display in the Event Capture pane. For more information about the Traffic Analysis pane and the Event Capture pane, see View Traffic Analytics and Events for a Traffic Rule on page 100.

Change a Traffic Rule

You can change any settings for an existing traffic rule.

To change the settings for a traffic rule:

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 **Traffic Controller**.
5. In the Traffic Rules pane, to the right of the rule, click the **pencil** icon.
   The Add Rule window opens.
6. Change the settings of the rule.
   For more information about the settings, see Add a Rule to Allow, Block, or Reject Traffic on page 93.
7. After you changed the settings, click **DONE**.
   The Traffic Rules table displays the changed settings for the rule.

Change the Action for a Traffic Rule

You can easily change the action for a traffic rule. For example, if the action for a rule is to block traffic, you can change it to allow traffic.

To change the action for a traffic rule:

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 **Traffic Controller**.
5. In the Traffic Rules pane, select one of the following actions from the menu for the rule in the Block column:

   - **Allow**. Allows traffic that conforms to the rule but blocks all other traffic.
   - **Block**. Blocks traffic that conforms to the rule but allows all other traffic. When traffic is blocked, it is dropped *without* notification to the traffic source.

     CAUTION: Make sure that your first traffic rule does not block all traffic for all devices because your connection to the router web interface might be terminated and you might need to reset the router to factory default settings to regain access.

   - **Reject**. Rejects traffic that conforms to the rule but allows all other traffic. When traffic is rejected, it is dropped *with* a notification to the traffic source. This action is available only for a rule that applies to all traffic or to a port range. It is not available for a rule that applies to particular categories of traffic or to specific games.

   The new action takes effect immediately.

Reorder the Priority of a Traffic Rule

The order of your traffic rules in the Traffic Rules table is important.

As you add rules, they are added to the table of rules, with the rule at the top of the table as the most important rule that takes priority over all other rules. The second rule in the table takes priority over all other rules that follow in the table, and so on. The rule at the bottom of the table is the least important rule that is applied only after all other rules were applied. However, you can reorder the rules in the table.

As an example, if you want to block every port except for one on your smart home device, set up a first rule that allows traffic on that one port on your smart home device. Then, set up a second rule that blocks all traffic on your smart home device.

To reorder the priority of a traffic rule:

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 **Traffic Controller**.
5. In the Traffic Rules pane, for the rule that you want to change, do the following:
   a. In the Priority column, to the right of the rule number, click and hold the icon with the six small dots.
   b. Move the rule up or down in the table, and release the icon where you want to place the priority of the rule.

   The rule and all rules below the rule are renumbered. The new priority takes effect immediately.

Enable or Disable a Traffic Rule

When you add a traffic rule, the rule is enabled automatically. You can disable the rule and you can enable it again.

To enable or disable a traffic rule:

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 **Traffic Controller**.
5. In the Traffic Rules pane, for the rule that you want to enable or disable, click the button in the Enabled column.

If the rule is disabled, the button displays white. If the rule is enabled, the button displays red.

The new action takes effect immediately.

Enable or Disable all Traffic Rules

When you add a traffic rule, the rule is enabled automatically. With one click of a button, you can disable all rules and you can enable them again.

To enable or disable all traffic rules:

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 **Traffic Controller**.
5. In the Traffic Rules pane, above the table, at the upper right, enable or disable all rules by clicking the **Disable All Rules** button.
   When all rules are disabled, the **Disable All Rules** button displays white. When all rules are enabled, the **Disable All Rules** button displays red.
   The new action takes effect immediately.

Enable or Disable Tracking for a Traffic Rule

When you add a traffic rule, you must decide whether event tracking is enabled (by default it is). After you add the rule, you can change the tracking settings.

To enable or disable tracking for a traffic rule:

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 **Traffic Controller**.
5. In the Traffic Rules pane, enable or disable tracking for a rule by selecting or clearing the check box in the Track column.

   If tracking is enabled for a rule, events for the rule display in the Event Capture pane. For more information about the Event Capture pane, see View Traffic Analytics and Events for a Traffic Rule on page 100.

   The new action takes effect immediately.

Remove a Traffic Rule

You can remove a traffic rule that you no longer need. After you remove the rule, traffic to which the rule applied is no longer affected.

To remove a traffic rule:

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 **Traffic Controller**.
5. In the Traffic Rules pane, to the right of the rule, click the **trashcan** icon.

   A confirmation window displays.

6. Click **Yes**.

   The rule is removed from the Traffic Rules table.

View Traffic Analytics and Events for a Traffic Rule

When you add a traffic rule, the router automatically provides traffic analytics for the rule. If event tracking is enabled for the rule, the router maintains a traffic rule event log. You can view this information.

To view traffic analytics and events a traffic rule:

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 **Traffic Controller**.
   In the Traffic Analytics pane and Event Capture pane, the following information displays:
   - **Traffic Analytics pane**. The information in this pane shows how effective your traffic rules are. The status indicator lights when traffic is being detected for the rule.
     For example, if a rule blocks all traffic for a device, the status indicator lights when the router detects that the device attempts to send or receive traffic. The number of packets and the number of bytes then increase to show the amount of traffic blocked by the rule.

     Note: Even when a traffic rule is disabled, you can monitor the potential effectiveness of the rule.

   - **Event Capture pane**. For each traffic rule for which event capturing is enabled, this pane includes an entry for each attempt to access blocked content and for each time allowed content was accessed. The information includes the services that were blocked or accessed and when they were blocked or accessed (that is, the events are timestamped).

Block Access to Internet Sites Using Keywords

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 Simple Outbound Firewall Rules on page 106.
   - **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 117).

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 Add Keywords and Block Access to Specific Internet Sites on page 101. 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 Simple Outbound Firewall Rules on page 106.
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 104.
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 Simple 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 Using Keywords on page 101), simple outbound firewall rules (see Block Services and Applications With Simple Outbound Firewall Rules on page 103), 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. 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 **Send to This 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 Alert Immediately** check box.

    Email alerts are sent immediately when someone attempts to visit a blocked site. This is the default setting.

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

    - **When log is full**. The router sends log messages when the log is full.
    - **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 selection from the menu is **None** and the router does not log messages.

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 112.
   - **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 42.
   - **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 114), 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 Feature 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 feature 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 123.

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 Setup 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 improve your network's capacity, Internet upload and download speeds, and WiFi range, keep the **Enable AX** check box selected.
   By default, AX WiFi is enabled. For more information about AX WiFi, see Enable or Disable AX WiFi on page 142.

Note: If AX WiFi is enabled, you can also enable Orthogonal Frequency-Division Multiple-Access (OFDMA) for each radio band independently. By default, OFDMA is disabled. For more information, see Enable or Disable OFDMA on page 142.

7. 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 disabled. If you select the **Enable Smart Connect** check box, the network name (SSID) and security option for the 5 GHz band are set to the same network name (SSID) and security option that are used in 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, keep the **Enable Smart Connect** check box cleared.

8. 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.

9. 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.

10. 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.

11. 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, in the 2.4 GHz radio band, 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 134. By default, the fastest modes are selected.

Note: For information about the options in the **Transmit Power Control** menu, see Change the Transmission Power Control on page 146.

Note: For information about the WiFi security settings in the Security Options section, see Change the WiFi Password or Security Level on page 132.

12. 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.

13. 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 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.

To change the Wi-Fi Protected Access (WPA) settings for the 2.4 GHz or 5 GHz radio:

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 Setup page displays.

5. In the Wireless Network (2.4GHz b/g/n/ax) section or the Wireless Network (5GHz a/n/ac/ax) section, under Security Options, select a WPA option:

   - **None**. With this option, the guest network does not provide WiFi security.

     Note: We recommend that you do not select this option. Make sure that your WiFi network is secured.

     WPA2-Personal [AES]. This is the default option. With this option, devices that support WPA2 and WPA3 can connect. The security of devices that support WPA3 is limited to the security that WPA2 supports.
   - **WPA-Personal [TKIP] + WPA2-Personal [AES]**. Use this option only if your network includes older devices that do not support WPA2. However, this modes limits the operation of the WiFi network in the 2.4 GHz radio band to 54 Mbps. The router is capable of much higher speeds.
   - **WPA3-Personal**. If all devices in your network support WPA3, use this mode because it supports the newest standard for the strongest security.

   The **Passphrase** field displays.

6. In the **Passphrase** field, enter the network key (password).
   For WPA2-Personal [AES] and WPA-Personal [TKIP] + WPA2-Personal [AES], this is a text string from 8 to 63 characters.

   For WPA3-Personal, this is a text string from 8 to 127 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).

The default WiF mode depends on whether the AX WiFi mode is enabled, which it is by default. For more information, see Enable or Disable AX WiFi on page 142.

Change the WiFi mode if AX WiFi is enabled

When AX WiFi is enabled (which it is by default), the router operates with up to 600 Mbps in the 2.4 GHz WiFi band and up to 4,800 Mbps in the 5 GHz WiFi band. You can select slower settings.

To change the WiFi mode settings if AX WiFi is enabled:

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 Setup page displays.

5. In the Wireless Network (2.4 GHz b/g/n/ax) section, select a WiFi mode from the **Mode** menu.
   - **Up to 600 Mbps**. This mode allows 802.11ax, 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11ax devices to function at up to 600 Mbps. This mode is the default mode.
   - **Up to 289 Mbps**. This mode allows for reduced interference with neighboring WiFi networks. This mode allows 802.11ax, 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11ax and 802.11n devices to functioning at up to 289 Mbps.
   - **Up to 54 Mbps**. This mode allows 802.11ax, 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11ax and 802.11n devices to functioning at up to 54 Mbps.
6. In the Wireless Network (5 GHz a/n/ac/ax) section, select a WiFi mode from the **Mode** menu.
   - **Up to 4800 Mbps**. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network and allows 802.11ax devices to function at up to 4800 Mbps. This mode is the default mode.
   - **Up to 2400 Mbps**. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network but limits 802.11ax devices to functioning at up to 2400 Mbps.
   - **Up to 1200 Mbps**. This mode allows for reduced interference with neighboring WiFi networks. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network but limits 802.11ax and 802.11ac devices to functioning at up to 1200 Mbps.
   - **Up to 600 Mbps**. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network but limits 802.11ax and 802.11ac devices to functioning at up to 600 Mbps.
7. Click the **Apply** button.
   Your settings are saved.

Change the WiFi mode if AX WiFi is disabled

When AX WiFi is disabled, the router operates with up to 400 Mbps in the 2.4 GHz WiFi band and up to 4,330 Mbps in the 5 GHz WiFi band. You can select slower settings.

To change the WiFi mode settings if AX WiFi is disabled:

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 Setup page displays.
5. In the Wireless Network (2.4 GHz b/g/n/ax) section, select a WiFi mode from the **Mode** menu.
   - **Up to 400 Mbps**. This mode allows 802.11ax, 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11ax devices to function at up to 400 Mbps. This mode is the default mode.
   - **Up to 173 Mbps**. This mode allows for reduced interference with neighboring WiFi networks. This mode allows 802.11ax, 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11ax and 802.11n devices to functioning at up to 173 Mbps.
   - **Up to 54 Mbps**. This mode allows 802.11ax, 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11ax and 802.11n devices to functioning at up to 54 Mbps.
6. In the Wireless Network (5 GHz a/n/ac/ax) section, select a WiFi mode from the **Mode** menu.
   - **Up to 4330 Mbps**. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network and allows 802.11ax devices to function at up to 4330 Mbps. This mode is the default mode.
   - **Up to 2165 Mbps**. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network but limits 802.11ax devices to functioning at up to 2165 Mbps.
   - **Up to 1000 Mbps**. This mode allows for reduced interference with neighboring WiFi networks. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a

devices to join the selected WiFi network in the 5 GHz band of the network but limits 802.11ax and 802.11ac devices to functioning at up to 1000 Mbps.

- **Up to 433 Mbps**. This mode allows 802.11ax, 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network but limits 802.11ax and 802.11ac devices to functioning at up to 433 Mbps.

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

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. In the Wireless Network (2.4GHz b/g/n/ax) - Profile section or the Wireless Network (5GHz a/n/ac/ax) - Profile section, under Security Options, select a WPA option:

   - **None**. This is the default selection. With this option, the guest network does not provide WiFi security.
   - **WPA2-Personal [AES]**. Use this option if your network includes devices that support WPA2. Devices that support WPA3 can connect too but their security is are limited to the security that WPA2 supports.
   - **WPA-Personal [TKIP] + WPA2-Personal [AES]**. Use this option only if your guest network includes older devices that do not support WPA2. However, this modes limits the operation of the guest WiFi network in the 2.4 GHz radio band to 54 Mbps. The router is capable of much higher speeds.
   - **WPA3-Personal**. If all devices in your guest network support WPA3, use this mode because it supports the newest standard for the strongest security.

   The **Passphrase** field displays.

10. In the **Passphrase** field, enter the network key (password).

    For WPA2-Personal [AES] and WPA-Personal [TKIP] + WPA2-Personal [AES], this is a text string from 8 to 63 characters.

    For WPA3-Personal, this is a text string from 8 to 127 characters.

11. 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.

12. Click the **Apply** button.

    Your settings are saved.

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 20 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 20 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.

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.

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.
   You can specify the settings for the 2.4 GHz band and 5 GHz band.
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.

Enable or Disable AX WiFi

AX WiFi improves your network's capacity, Internet upload and download speeds, and WiFi range by allowing WiFi traffic from different devices to be concurrently managed. To do this, AX WiFi uses 4x4 multi-user MIMO and intelligent scheduling and can use Orthogonal Frequency-Division Multiple-Access (OFDMA).

AX WiFi is enabled by default.

To enable or disable AX WiFi:

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 Setup page displays.
5. Select or clear the **Enable AX** check box.
   Selecting this check box turns on AX WiFi and clearing this check box turns off AX WiFi.
6. Click the **Apply** button.
   Your settings are saved.

Enable or Disable OFDMA

If AX WiFi is enabled (which it is by default), you can enable Orthogonal Frequency-Division Multiple-Access (OFDMA) for each radio band independently. By default, OFDMA is disabled in both radio bands, even when AX WiFi is enabled.

OFDMA allows data transmission signals to be split into smaller signals. Your router sends these small signals directly to individual devices in your network. Because multiple devices can be served in the same transmission window, your router doesn't have to

wait for medium access for every packet. This method of communication increases network speed and efficiency.

Note the following about OFDMA:

- Enable OFDMA if your network includes many Internet of things (IoT) devices.
- After you enable OFDMA, if you notice that some of your devices do not function as expected, disable OFDMA to see if the devices function fine.
- If your network includes many older devices, you might want to keep OFDMA disabled.

To enable or disable OFDMA:

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 Setup page displays.
5. Select or clear the **Enable OFDMA in 2.4GHz** check box.
   Selecting this check box turns on OFDMA in the 2.4 GHz radio band and clearing this check box turns off OFDMA in the 2.4 GHz radio band.
6. Select or clear the **Enable OFDMA in 5GHz** check box.
   Selecting this check box turns on OFDMA in the 5 GHz radio band and clearing this check box turns off OFDMA in the 5 GHz radio band.
7. Click the **Apply** button.
   Your settings are saved.

Enable or Disable Smart Connect

Smart Connect selects the fastest WiFi band for your device. For Smart Connect to work, the 2.4 GHz and 5 GHz bands must use the same WiFi network name (SSID) and network

key (password). 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 WiFi settings for 2.4 GHz band overwrites the WiFi settings for 5 GHz band.

To enable or disable Smart Connect:

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 Setup page displays.
5. Select or clear the **Enable Smart Connect** check box.
   Selecting this check box turns on Smart Connect and clearing this check box turns off Smart Connect.
6. Click the **Apply** button.
   Your settings are saved.

Manage Implicit Beamforming

Implicit beamforming contrasts with explicit beamforming, which means the router actively tracks clients and directs power to the router antenna closest to the client. Explicit beamforming works whether or not the client supports beamforming. Implicit beamforming means that the router can use information from client devices that support beamforming to improve the WiFi speed, reliability, and range. This feature is enabled by default, but you can disable it.

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.

Enable or Disable 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 disabled by default, but you can enable it.

To enable or 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 select or 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.

Change the Transmission Power Control

By default, you router's transmission power is set to 100%. This allows your router to give you whole home WiFi coverage. If you don't need whole home WiFi coverage, and you also want to save power consumption while using your router, you can lower the transmission power of your router.

To change the transmission power control:

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 Setup page displays.
   You can specify the settings for the 2.4 GHz band and 5 GHz band.
5. In the Wireless Network (2.4 GHz b/g/n) section, select a percentage from the **Transmit Power Control** menu.
6. In the Wireless Network (5 GHz a/n/ac) section, select a percentage from the **Transmit Power Control** menu.
7. 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 Game Servers and Your Devices, Router, and Network on page 74.

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. By default, the router automatically updates to future firmware as they become available so that your router is up to date with the latest features and security fixes. (If you prefer the router to not automatically update to future firmware, you can disable the option.)

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 prevent the router from automatically updating to future firmware versions, do the following:
   a. Select **Settings > Administration > Firmware Update**.
      The Firmware Update page displays.
   b. In the Router Auto Firmware Update section, select the **Disable** 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 Recovery

The router admin password is used to log in to your router web interface. We recommend that you enable password recovery if you change the router admin password. Then you can recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers but not in the Safari browser.

To enable password recovery:

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. Select the **Enable Password Recovery** check box.
6. Select two security questions and provide answers to them.
7. Click the **Apply** button.
   Your settings are saved.

Recover the admin Password

If you set up the password recovery feature, you can recover your router admin password.

To recover your router admin password:

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. Click the **Cancel** button.
   If password recovery 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.
   A window opens requesting the answers to your security questions.
6. Enter the saved answers to your security questions.
7. Click the **Continue** button.
   A window opens and displays your recovered password.
8. Click the **Login again** button.
   A login window opens.
9. With your recovered password, log in to the 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.

Return the Router to its Factory Default Settings

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

To reset the router to factory default settings, you can use either the **Reset** button on the back of the router or the erase function. in the router web interface.

After you reset the router to factory default settings, the user name is admin, the password is password, the LAN IP address is 192.168.1.1 (which is the same as www.routerlogin.net), and the DHCP server is enabled.

Tip: If the router is in access point mode or bridge mode and you do not know the IP address that is assigned to it, first try to use an IP scanner application to detect the IP address. (IP scanner applications are available online free of charge.) If you can detect the IP address, you don't need to reset the router to factory default settings.

Use the Reset button

To reset the router to factory default settings:

1. On the back of the router, locate the **Reset** button.
2. Using a straightened paper clip, press and hold the **Reset** button for at least five seconds.
3. Release the **Reset** button.

   The Power LED starts blinking. When the reset is complete, the router restarts. This process takes about two minutes.

   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.

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.

Set Your Time Zone

To set your time zone:

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 > NTP**.
   The NTP Settings page displays.
5. Select your time zone from the menu.
6. If you live in a region that observes daylight saving time, select the **Automatically adjust for daylight savings time** check box.
7. Click the **Apply** button.
   Your settings are saved.

Change the NTP Server

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

To change the NTP server to your preferred NTP server:

1. Launch a web browser from a computer or mobile device that is connected to the 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 > NTP** .
   The NTP Settings page displays.
5. Select the **Set your preferred NTP server** radio button.
6. Enter the NTP server domain name or IP address in the **Primary NTP server** field.
7. Click the **Apply** button.
   Your settings are saved.

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 161.

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 161.

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 161.

View the Internet Traffic Volume and Statistics

If you enabled the traffic meter (see Start the Traffic Meter Without Traffic Volume Restrictions on page 158), you can view the Internet traffic volume and statistics.

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

1. Launch a web browser from a computer or mobile device that is connected to the 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 Logs of Router Activity

The logs are a detailed record of the websites you accessed or attempted to access and many other router actions. Up to 256 entries are stored in the log.

To view and manage logs:

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 > Logs**.
   The Logs page displays and shows information such as the following:
   - **Action**. The action that occurred, such as whether Internet access was blocked or allowed.
   - **Source IP**. The IP address of the initiating device for the log entry.
   - **Target address**. The name or IP address of the website or news group visited or to which access was attempted.
   - **Date and time**. The date and time the log entry was recorded.

   Other information might be displayed.
5. To customize the logs, scroll down and clear or select the check boxes in the Include in Log section.
6. To refresh the log screen, click the **Refresh** button.
7. To clear the log entries, click the **Clear Log** button.

   Note: Before you clear the log entries, we recommend that you email the log entries (see the next step).

8. To email the log immediately, click the **Send Log** button.
   You must set up email notifications in order to receive the logs. The router to emails the logs to the address that you specified when you set up email notifications. For

more information, see Set Up Email Notifications for Security Events and Log Messages on page 107.

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

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 **Settings > Administration > Reboot**.

   The Reboot page displays.
5. 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 the Media Server

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

You can disable the media server, for example, if another device on your network already functions as a media server.

Note: For information about changing the media server name, see Change the Router's Device Name on page 113.

To disable the media 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 > USB Functions > Media Server**.
   The Media Server (Settings) page displays.
5. Clear the **Enable DLNA Media Server** check box.
6. Click the **Apply** button.
   Your settings are saved.

Turn Off the Router LEDs

The LEDs on the top panel of the router indicate activities and behavior. You can turn off all LEDs except the Power LED.

To turn off the LEDs:

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. To turn off all LEDs except the Power LED, select the **Turn off all LEDs except Power LED** radio button.
6. Click the **Apply** button.
   Your settings are saved.

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 149.

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

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+

Access a storage device connected to the router

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

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.

Manage Access to a USB Storage Device

You can manage how you access a USB storage device that is connected to the router.

To manage the USB 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 Functions > 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 Use Dynamic DNS to Access USB Storage Devices Through the Internet on page 180), 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.

   Note: We strongly recommend that you enable Admin Password Protection to secure your ReadySHARE data.

   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 Your Network

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

For information about using FTP over the Internet, see Set Up Your Personal FTP Server on page 183.

To set up FTP access within your 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 > USB Functions > 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 Functions > 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 Functions > 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 Functions > 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.

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 Functions > 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 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.

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 181.
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 185.
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 186.

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.

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 181.
   - 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 Functions > 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 185).

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

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**.

13

Use VPN to Access Your Network

You can use OpenVPN software to remotely access your router using virtual private networking (VPN). This chapter describes how to set up VPN service in the router and use VPN access.

The chapter includes the following sections:

Set Up a VPN Connection

A virtual private network (VPN) lets you use the Internet to securely access your network when you are not home.

This type of VPN access is called a client-to-gateway tunnel. The computer is the client, and the router is the gateway that provides the VPN service. To use the VPN feature, you must log in to the router and enable VPN, and you must install and run VPN client software on the computer.

VPN uses DDNS or a static IP address to connect with your router.

To use a DDNS service, register for an account with a host name (sometimes called a domain name). You use the host name to access your network. The router supports these accounts: NETGEAR, No-IP, and Dyn. For more information, see Set Up and Manage Dynamic DNS on page 181.

If your Internet service provider (ISP) assigned a static WAN IP address (such as 50.196.x.x or 10.x.x.x) that never changes to your Internet account, the VPN can use that IP address to connect to your home network.

Specify VPN Service in the Router

You must specify the VPN service settings in the router before you can use a VPN connection to the router.

To specify the VPN 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 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 Service**.
   The VPN Service page displays.
5. Select the **Enable VPN Service** check box.
   By default, the VPN uses the UDP service type with port 12973 for TUN mode service and port 12974 for TAP mode service. If you want to customize the service type and

port, we recommend that you change these settings before you install the OpenVPN software.

6. To change the service type, scroll down and select the **TCP** radio button.
7. To change the port numbers, scroll down to the **Service Port** fields, and type the port numbers that you want to use.

   Note: By default, the **Auto** radio button is selected, which lets the router use an automatic detection system that enables VPN access only for necessary services and sites and might not include full Internet access. For information about the other options, see Allow VPN Client Internet Access in the Router on page 201 and Block VPN Client Internet Access in the Router on page 202.

8. Click the **Apply** button.

   Your settings are saved. VPN is enabled in the router, but you must install and set up OpenVPN software on your computer before you can use a VPN connection.

Install OpenVPN Software

You must install this software on each Windows-based computer, Mac computer, iOS device, or Android device that you plan to use for VPN connections to your router.

Install OpenVPN Software on a Windows-Based Computer

You must install OpenVPN software on each computer that you plan to use for VPN connections to your router.

To install VPN client software on a Windows-based 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 > Advanced Settings > VPN Service**.

   The VPN Service page displays.

5. If you did not yet enable VPN service, select the **Enable VPN Service** check box and click the **Apply** button.

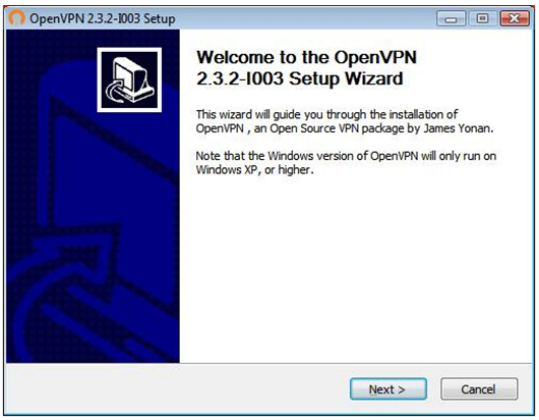
   Your settings are saved.

   For information about the advanced configuration options on this page, see Specify VPN Service in the Router on page 193.

6. Click the **For Windows** button to download the OpenVPN configuration files.

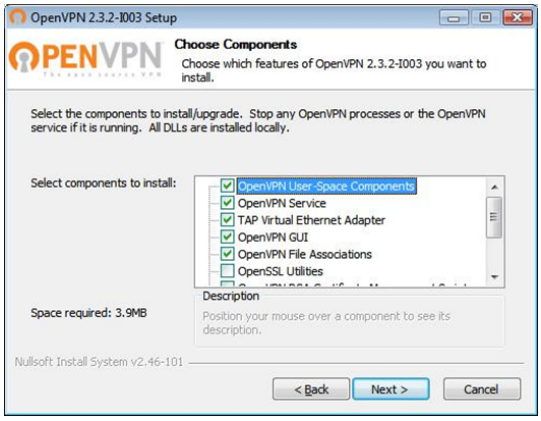
   Step 17 provides information about what to do with the downloaded OpenVPN configuration files.

7. To download the OpenVPN client utility, visit openvpn.net/index.php/download/community-downloads.html.
8. In the Windows Installer section of the page, double-click the **openVPN-install-xxx.exe** link.
9. Download the file.
10. To install the OpenVPN client utility on your computer, click the **openVPN-install-xxx.exe** file.



11. Click the **Next** button.

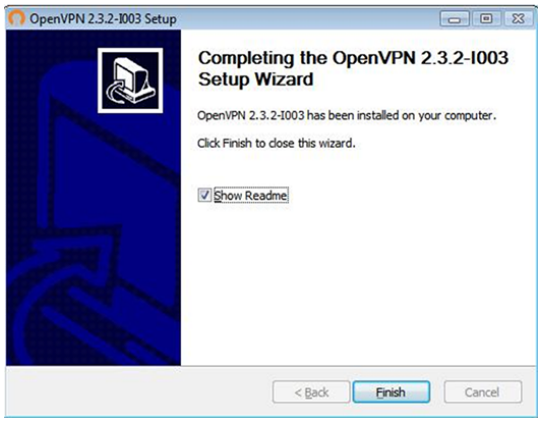
12. Read the License Agreement and click the **I Agree** button.



13. Leave the check boxes selected as shown in the previous figure, and click the **Next** button.
14. To specify the destination folder, click the **Browse** button, select a destination folder, and click the **Next** button.

15. Click the **Install** button.

    The window displays the progress of the installation and then displays the final installation window.



16. Click the **Finish** button.
17. Unzip the configuration files that you downloaded in Step 6 and copy them to the folder in which the OpenVPN client utility is installed on your computer.

If your device is a Windows 64-bit system, the OpenVPN client utility is installed by default in the `C:\Program files\OpenVPN\config\` folder.

18. Modify the VPN interface name to **NETGEAR-VPN**:
    a. On your computer, go to the Networks window. If you are using Windows 10, select **Control Panel > Network and Sharing Center > Change 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.

For more information about using OpenVPN on a Windows-based computer, visit openvpn.net/index.php/open-source/documentation/howto.html#quick.

Install OpenVPN Software on Your Mac Computer

You must install this software on each Mac computer that you plan to use for VPN connections to your router.

To install VPN client software on your Mac 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 > Advanced Settings > VPN Service**.
   The VPN Service page displays.
5. If you did not yet enable VPN service, select the **Enable VPN Service** check box and click the **Apply** button.
   Your settings are saved.
   For information about the advanced configuration options on this page, see Specify VPN Service in the Router on page 193.

6. Click the **FOR MACOSX** button to download the OpenVPN configuration files.
7. Visit https://tunnelblick.net/index.html to download the OpenVPN client utility for Mac OS X.
8. Download and install the file.
9. Unzip the configuration files that you downloaded and copy them to the folder where the VPN client is installed on your device.

   The client utility must be installed by a user with administrative privileges.

   For more information about 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 this software on each iOS device that you plan to use for VPN connections to your router.

To install VPN client software on an iOS 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 **Settings > Advanced Settings > VPN Service**.

   The VPN Service page displays.
5. If you did not yet enable VPN service, select the **Enable VPN Service** check box and click the **Apply** button.

   Your settings are saved.

   For information about the advanced configuration options on this page, see Specify VPN Service in the Router on page 193.
6. Click the **For Smart Phone** button to download the OpenVPN configuration files.
7. On your iOS device, download and install the OpenVPN Connect app from the Apple App Store.
8. On your computer, unzip the configuration files that you downloaded and send the files to your iOS device.

Note that when you open the .ovpn file, a list of apps displays. Select the OpenVPN Connect app to open the .ovpn file.

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

Install OpenVPN Software on an Android Device

You must install this software on each Android device that you plan to use for VPN connections to your router.

To install VPN client software on an Android 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 **Settings > Advanced Settings > VPN Service**.
   The VPN Service page displays.
5. If you did not yet enable VPN service, select the **Enable VPN Service** check box and click the **Apply** button.
   Your settings are saved.
   For information about the advanced configuration options on this page, see Specify VPN Service in the Router on page 193.
6. Click the **For Smart Phone** button to download the OpenVPN configuration files.
7. On your Android device, download and install the OpenVPN Connect app from the Google Play Store.
8. On your computer, unzip the configuration files that you downloaded and send the files to your Android device.
9. Open the files on your Android device.
10. Open the .ovpn file using the OpenVPN Connect app.
    For more information about using OpenVPN on your Android device, visit http://www.vpngate.net/en/howto_openvpn.aspx#android.

Use a VPN Tunnel on a Windows-Based Computer

After you set up the router to use VPN and install the OpenVPN application on a Windows-based computer, you can open a VPN tunnel from your computer to your router over the Internet.

For the VPN tunnel to work, the local LAN IP address of the remote router must use a different LAN IP scheme from that of the local LAN where your VPN client computer 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.

The default LAN IP address scheme for the router is 192.x.x.x. The most common IP schemes are 192.x.x.x, 172.x.x.x, and 10.x.x.x. If you experience a conflict, change the IP scheme either for your home network or for the network with the client VPN computer. For information about changing these settings, see Change the Router's LAN IP Address and RIP Settings on page 114.

To open a VPN tunnel on a Windows-based computer:

1. Launch the OpenVPN application with administrator privileges.
   The OpenVPN icon displays in the Windows taskbar.

   Tip: You can create a shortcut to the VPN program, then use the shortcut to access the settings and select the **run as administrator** check box. Then every time you use this shortcut, OpenVPN automatically runs with administrator privileges.

2. Right-click the **OpenVPN** icon and select **Connect**.
   The VPN connection is established. You can do the following:

   - Launch a web browser and log in to your router.
   - Use Windows file manager to access the router's USB device and download files.

Use VPN to Access the Router's USB Storage Device and Media

To use a Windows-based computer to access a USB storage device that is attached to the router and download files:

1. Open File Explorer or Windows Explorer and select **Network**.
   The network resources display. The **ReadySHARE** icon is in the Computer section and the remote router icon is in the Media Devices section (if DLNA is enabled in the router).
2. If the icons do not display, click the **Refresh** button to update the windows.
   If the local LAN and the remote LAN are using the same IP scheme, the remote router icon does not display in the Media Devices and Network Infrastructure sections.
3. To access the USB device, click the **ReadySHARE** icon.
4. To access media on the router's network, click the remote router icon.

Use VPN to Access Your Internet Service at Home

When you are 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.

Then router lets you use a VPN connection to access your own Internet service when you are away from home. You might want to do this if you travel to a geographic location that does not support all the Internet services that you use at 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, VPN service in the router uses the Auto option, which lets the router use an automatic detection system that enables VPN access only for necessary services and sites and might not include full Internet access. You can change the settings to allow

access to your home network and the Internet. 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 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 Service**.
   The VPN Service page displays.
5. If you did not yet enable VPN service, select the **Enable VPN Service** check box and click the **Apply** button.
   Your settings are saved.
   For information about the advanced configuration options on this page, see Specify VPN Service in the Router on page 193.
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 only.
7. Click the **Apply** button.
   Your settings are saved.

   Note: For information about downloading and installing the configuration files for your VPN clients, see Install OpenVPN Software on page 194.

Block VPN Client Internet Access in the Router

By default, VPN service in the router uses the Auto option, which lets the router use an automatic detection system that enables VPN access only for necessary services and sites and might not include full Internet access. You can change the settings to allow access to your home network only and block access to the Internet.

To allow VPN clients to access your home network only:

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 Service**.
   The VPN Service page displays.
5. If you did not yet enable VPN service, select the **Enable VPN Service** check box and click the **Apply** button.
   Your settings are saved.
   For information about the advanced configuration options on this page, see Specify VPN Service in the Router on page 193.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **Home Network only** radio button.
   The VPN connection is to your home network only, *not* to the Internet service for your home network.
7. Click the **Apply** button.
   Your settings are saved.

   Note: For information about downloading and installing the configuration files for your VPN clients, see Install OpenVPN Software on page 194.

Use a VPN Tunnel to Access Your Internet Service at Home

To access your Internet service:

1. Set up the router to allow VPN access to your Internet service.
   See Use a VPN Tunnel to Access Your Internet Service at Home on page 203.
2. On your computer, launch the OpenVPN application.
   The **OpenVPN** icon displays in the Windows taskbar.
3. Right-click the icon and select **Connect**.

4. When the VPN connection is established, launch your Internet browser.

14

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 112).

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 117.

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 207.
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 **Service Type** menu, select the protocol.
   If you are unsure, select **TCP/UDP**.

9. In the **External Starting Port** field, type the default port number for the service or application.
10. In the **External Ending Port**, type the same port number, or, for each additional computer that uses the service or application, increase the port number with one digit.

    For example, if you configure one computer to use a service or application using port 26900 and you want to set up two additional computers, type 26902 in the field. The port number for the first computer is 26900, for the second one it is 26901, and for the third one it is 26902.

11. 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 in the **Internal Starting Port** and **Internal Ending Port** fields.

12. In the **Internal IP address** field, type the IP address or select the radio button for an attached device listed in the table.
13. 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 207.
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 181) 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 127.

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 212.

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 211), 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 211.
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.

15

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 83).

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 Off the Router LEDs on page 168).

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 Off the Router LEDs on page 168).

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, and 5 GHz 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 Off the Router LEDs on page 168).

The WiFi LED, 2.4 GHZ LED, and 5 GHz LED light when the WiFi radios are turned on.

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 165.

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 162.
- 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 Off the Router LEDs on page 168).
- 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 130). 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 225.
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.

16

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 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 600 Mbps 5 GHz: Up to 4800 Mbps
	Fragmentation Length	2346
	CTS/RTS threshold	2347
	Preamble mode	Long Preamble
	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
	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, Dynamic DNS, and UPnP
Power adapter input	North America: 100–240V, 50/60 Hz AC Australia: 220–240V, 50/60 Hz AC Europe: 100–240V, 50/60 Hz AC
Power adapter output	12V/2.5A DC
Dimensions	11.61 x 7.87 x 2.51 in. (295 x 200 x 64 mm)
Weight	1.32 lb (600 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	One USB 3.0 port
Wireless	Maximum WiFi signal rate complies with the IEEE 802.11 standard. **Note**: 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.
Radio data rates	Auto-rate sensing
Data encoding standards	IEEE 802.11b/g/n 2.4 GHz 256 QAM support IEEE 802.11ax 2.4 GHz 1024 QAM support IEEE 802.11a/n/ac 5.0 GHz 256 QAM support IEEE 802.11ax 5.0 GHz at 80 MHz 1024 QAM support **Note**: NETGEAR makes no express or implied representations or warranties about this product's compatibility with any future standards.
Maximum WiFi clients per WiFi network	Limited by the amount of WiFi network traffic generated by each client (typically 50–70 clients)
2.4 GHz band operating frequency range	US: 2.412–2.462 GHz Europe: 2.412–2.472 GHz Australia: 2.412–2.472 GHz Japan: 2.412–2.472 GHz

Table 4. Router technical specifications (Continued)

Feature	Description
5 GHz band operating frequency range	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-Personal [AES] WPA-Personal [TKIP] + WPA2-Personal [AES] (mixed mode) WPA3-Personal **Note**: Legacy WEP is supported for bridge mode only.

Note: For more information, see the data sheet, which is available at netgear.com/support/download.