NETGEAR®

User Manual

AC1600 Smart WiFi Router

Model R6260

March 2020
202-11818-03

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 Performance

Chapter 5 Manage the Basic WiFi Network Settings

Chapter 6 Control Access to the Internet

Chapter 7 Share USB Storage Devices Attached to the Router

Chapter 8 Use Dynamic DNS to Access USB Storage Devices Through the Internet

Chapter 9 Use the Router as a Media Server

Chapter 10 Manage the WAN and LAN Network Settings

Chapter 11 Manage Your Router

Chapter 14 Manage Port Forwarding and Port Triggering

Chapter 15 Troubleshooting

Appendix A Supplemental Information

1

Hardware Overview of the Router

This chapter contains the following sections:

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

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

Unpack Your Router

Your package contains the router, power adapter, and an Ethernet cable.

Figure 1. Package contents

In some regions, a CD is included in the package.

LEDs and Buttons on the Top Panel

The status LEDs and buttons are located on the top of the router.

Table 1. LED and button descriptions

LED and Button	Description
Power	**Solid green**. The power is on and the router is ready. **Blinking green**. A firmware update is in progress. **Off**. Power is not supplied to the router.
Internet	**Solid green**. The Internet connection is ready. **Off**. No Ethernet cable is connected between the router and the modem.

Table 1. LED and button descriptions (Continued)

LED and Button	Description
WiFi	**Solid green**. The WiFi radio is operating. **Off**. The WiFi radios are off.
USB	**Solid green**. A USB device is connected and is ready. **Off**. No USB device is connected.

Ports, Buttons, and Connectors on the Back Panel

The back panel of the router provides ports, buttons, antenna connectors, and a DC power connector.

Figure 2. Router back panel

In addition to the two antenna connectors, viewed from left to right, the back panel contains the following components:

- **USB port**. Use the USB 2.0 port to connect USB devices.
- **Ethernet LAN ports**. Use the four Gigabit Ethernet RJ-45 LAN ports to connect the router to LAN devices.
- **WAN port**. Use the yellow Gigabit Ethernet RJ-45 WAN port to connect the router to a modem.
- **WPS button**. Use this button to connect WPS-enabled devices to the router.

- **Reset button**. For information about using the **Reset** button, see Return the router to its factory default settings on page 141.
- **Power On/Off button**. Press the **Power On/Off** button to provide power to the router.
- **DC power connector**. Connect the power adapter that came in the product package to the DC power connector.

Router Label

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

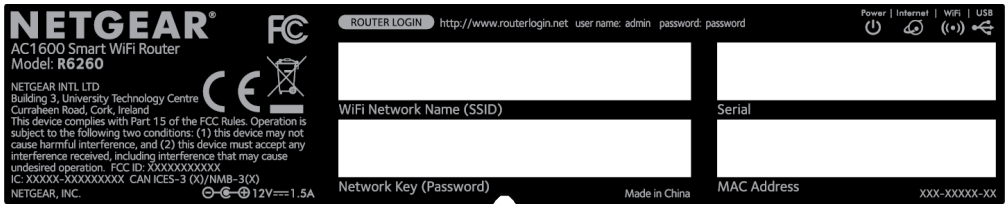


Figure 3. Router label

Position the 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 the router. For example, the thickness and number of walls the WiFi signal passes through can limit the range.

Additionally, other WiFi access points in and around your home might affect your router's signal. WiFi access points are routers, repeaters, WiFi range extenders, and any other device that emits a WiFi signal for network access.

Position the router according to the following guidelines:

- Place the router near the center of the area where your computers and other devices operate and within line of sight to your WiFi devices.
- Make sure that the router is within reach of an AC power outlet and near Ethernet cables for wired computers.
- Place the router in an elevated location, minimizing the number walls and ceilings between the router and your other devices.

- Place the router away from electrical devices such as these:
  - Ceiling fans
  - Home security systems
  - Microwaves
  - Computers
  - Base of a cordless phone
  - 2.4 GHz cordless phone
  - 5 GHz cordless phone
- Place the router away from large metal surfaces, large glass surfaces, insulated walls, and items such as these:
  - Solid metal door
  - Aluminum studs
  - Fish tanks
  - Mirrors
  - Brick
  - Concrete

If you are using adjacent access points, use different radio frequency channels to reduce interference.

Cable Your Router

The following image shows how to cable your router:

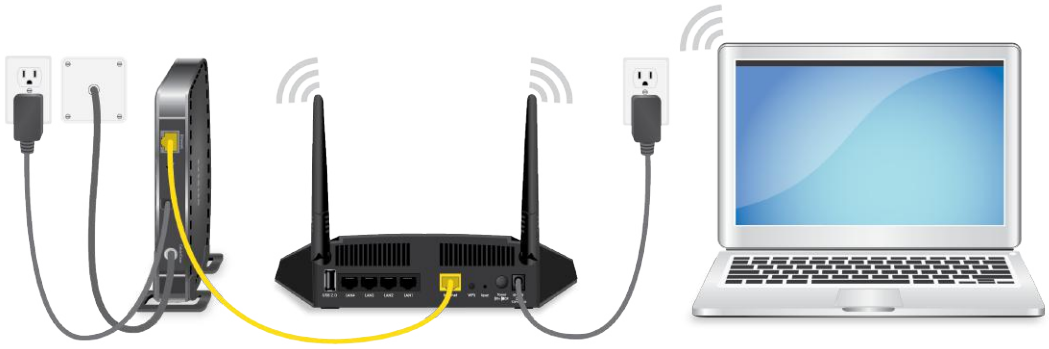


Figure 4. Router cabling

To cable your router:

1. Unplug your modem's power, leaving the modem connected to the wall jack for your Internet service.
   If your modem uses a battery backup, remove the battery.
2. Plug in and turn on your modem.
   If your modem uses a battery backup, put the battery back in.
3. Connect your modem to the Internet port of your router with the yellow Ethernet cable that came with your router.
4. Connect the power adapter to your router and plug the power adapter into an outlet.
5. Press the **Power On/Off** button on the back panel of the router.

Wall-Mount Your Router

Wall-mounting holes on the bottom wall-mount your router.

Figure 5. Bottom of the router

Note: We recommend using pan head Phillips wood screws, 3.5 x 20 mm (diameter x length, European) or No. 6 type screw, 1 inch long (U.S.).

To wall-mount your router:

1. Drill holes in the wall where you want to wall-mount your router.
2. Insert wall anchors in the holes.
3. Insert screws into the wall anchors, leaving 3/16 in (0.5 cm) of each screw exposed.
4. Align the router's wall-mounting holes with the screws and mount your router.

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 explains the ways you can connect and how to access the router and log in.

The chapter contains the following sections:

Connect to the network

You can connect to the router's network through a wired or WiFi connection. 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 network 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 a LAN port on the router.
   Your computer connects to the local area network (LAN).

Find and connect to the WiFi network

To find and select the WiFi network:

1. Make sure that the router is receiving power (its Power LED is lit).
2. On your computer or WiFi device, find and select the WiFi network.
   The WiFi network name is on the router label.
3. Join the WiFi network and enter the WiFi password.
   The password is on the router label.

   Your device connects to the WiFi network.

WiFi connection using WPS

You can connect your WPS-enabled device 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 WPS-enabled device.
3. Press the **WPS** button on the router.

4. Within two minutes, on your WPS-enabled device, press its **WPS** button or follow its instructions for WPS connections.

   Your WPS-enabled device connects to the WiFi network.

Types of logins

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

Several types of logins are associated with the router:

- **ISP login**. The login that your Internet service provider (ISP) gave you logs you in to your Internet service. Your ISP gave you this login information in a letter or some other way. If you cannot find this login information, contact your ISP.
- **WiFi network key, WiFi passphrase, or WiFi password**. Your router is preset with a unique WiFi network name (SSID) and password for WiFi access. This information is on the router label.
- NETGEAR account login. The free NETGEAR account that you need to register your router and manage your subscriptions. If you do not own a NETGEAR account, you can create one.
- **Router login**. The router login password that you need to log in to the router with the admin user name when you use a web browser to access the router.

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.

The NETGEAR installation assistant runs on any device with a web browser. Installation and basic setup takes about 15 minutes to complete.

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 onscreen instructions.

   The router connects to the Internet.

5. If the browser does not display the NETGEAR installation assistant, 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 193. If problems persist, register your NETGEAR product and contact NETGEAR Technical Support.

Log in to the router

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

Install and manage your router with the Nighthawk app

With the Nighthawk app, you can easily install and manage your router. The app automatically updates the router to the latest firmware, allows you to personalize your WiFi network, and even helps register your router with NETGEAR.

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

To install your router using the Nighthawk app:

1. To download the app, visit Nighthawk-app.com.
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 (WiFi password) are on the router label.

   If the label includes a QR code, you can scan the QR code to join the router's WiFi network.
3. Launch the Nighthawk app on your mobile device.
4. Follow the prompts on the app to install your router and connect to the Internet.

Change the language

By default, the language that displays when you log in to the router web interface is set to Auto.

To change the language:

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

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

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

   The BASIC Home page displays.
4. In the upper right corner, select a language from the menu.
5. When prompted, click the **OK** button to confirm this change.

   The page refreshes with the language that you selected.

3

Specify Your Internet Settings

Usually, the quickest way to set up the router to use your Internet connection is to allow your router to detect the Internet connection automatically when you first access the router web interface. You can also customize and manually 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 BASIC Home page displays.
4. Select **ADVANCED > Setup Wizard**.
   The Setup Wizard page displays.
5. Select the **Yes** radio button.
   If you select the **No** radio button, you are taken to the Internet Setup page (see Manually set up the Internet connection on page 25).
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 therouter network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.

3. Enter the router admin user name and password.

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

   The BASIC Home page displays.

4. Select **Internet**.

   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 193.

Specify an Internet connection that uses a login and PPPoE service

You can manually specify the connection settings for a PPPoE Internet service for which you must log in. Use the information that your Internet service provider (ISP) gave you to connect to your Internet service. If you cannot find this information, contact your ISP. Entering incorrect information might prevent the router from connecting to the Internet.

To specify the connection settings for a PPPoE Internet service for which you must log in:

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

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

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

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

   The Internet Setup page displays.
5. Select the Does your Internet connection require a login? **Yes** radio button.

   The page adjusts.
6. From the **Internet Service Provider** menu, select **PPPoE** as the encapsulation method.

   The page adjusts.
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 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 193.

Specify an Internet connection that uses a login and PPTP or L2TP service

You can manually specify the connection settings for a PPTP or L2TP Internet service for which you must log in. Use the information that your Internet service provider (ISP) gave you to connect to your Internet service. If you cannot find this information, contact

your ISP. Entering incorrect information might prevent the router from connecting to the Internet.

To specify the connection settings for a PPTP or L2TP Internet service for which you must log in:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **Internet**.
   The Internet Setup page displays.
5. Select the Does your Internet connection require a login? **Yes** radio button.
   The page adjusts.
6. From the **Internet Service Provider** menu, select **PPTP** or **L2TP** as the encapsulation method.
   The page adjusts.
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. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.
10. 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 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.
11. If your ISP gave you fixed IP addresses and a connection ID or name, type them in the **My IP Address**, **Subnet Mask**, **Server Address**, **Gateway IP Address**, and **Connection ID/Name** fields.
    If your ISP did not give you IP addresses, a connection ID, or name, leave these fields blank. The connection ID or name applies to a PPTP service only.

12. Select a Domain Name Server (DNS) Address radio button:
    - **Get Automatically from ISP**. Your ISP uses DHCP to assign 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.
13. 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.
14. Click the **Apply** button.
    Your settings are saved.
15. Click the **Test** button to test your Internet connection.
    If the NETGEAR website does not display within one minute, see You cannot access the Internet on page 193.

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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > 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.

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

Your Internet service provider (ISP) can provide this information.

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 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Config**.
   The page adjusts.
   The 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**. 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.

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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Detect**.
   The page adjusts.
   The 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.

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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **6to4 Tunnel**.
   The page adjusts.
   The 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**. 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 6rd Tunnel Connection

The 6rd protocol makes it possible to deploy IPv6 to sites 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 that is 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, enabling stateless operation of 6rd.

To set up an IPv6 6rd tunnel 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 user name and password.

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

   The BASIC Home page displays.

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

5. From the **Internet Connection Type** menu, select **6rd 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. In the 6rd Configuration section, configure the 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 Border Relay Address**. Enter the border router's IPv4 address that your ISP gave you.
   - **6rd 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 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 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Pass Through**.
   The page adjusts, but no additional fields display.
6. Click the **Apply** button.
   Your settings are saved.

Set up a fixed IPv6 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
   The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Fixed**.
   The page adjusts.
6. 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 25.)
7. 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).
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 BASIC Home page displays.

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

   The IPv6 page displays.

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

   The page adjusts.

   The 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**. 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.

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

   The page adjusts.

   The 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. 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.

7. In the **Password** field, enter the password for the ISP connection.
8. 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.

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

   - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns 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 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).

11. (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.

12. Click the **Apply** button.

    Your settings are saved.

Manage the MTU size

The maximum transmission unit (MTU) is the largest data packet a network device transmits.

MTU concepts

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 maximum transmission unit (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 Internet service, and the technical support of either the Internet service provider (ISP) or NETGEAR recommends changing the MTU setting.
  For example, if a secure website does not open, or displays only part of a web page, you might need to change the MTU.
- 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.

CAUTION: 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.

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.

Table 2. Common MTU sizes (Continued)

MTU	Application
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1458	Used in PPPoA environments.
1436	Used in PPTP environments or with VPN.

Change the MTU size

WARNING: An incorrect MTU setting can cause Internet communication problems. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers. Change the MTU only if you are sure that it is necessary for your ISP connection.

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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. In the **MTU Size** field, enter a value from 64 to 1500.
   The normal maximum transmit unit (MTU) value for most Ethernet networks is 1500 bytes, 1492 bytes for PPPoE connections, or 1436 for PPTP connections.
6. Click the **Apply** button.
   Your settings are saved.

4

Optimize Performance

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

The chapter contains the following sections:

Optimize Traffic With QoS

You can use Quality of Service (QoS) to assign different priorities to Internet traffic, applications, and services. The router provides default QoS rules. You can add custom QoS rules and manage both default and custom QoS rules (see Manage Default and Custom QoS Rules on page 46).

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

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.
   If you did not add any custom rules or change priorities, the QoS rules table displays the default QoS rules and their default priority queues, from the highest queue (the leftmost column) to the lowest priority (the rightmost column).
5. Select the **Turn Internet Access QoS On** check box.
6. Click the **Apply** button.
   Your settings are saved. The router assigns traffic priorities according to the QoS rules and their priority queues.

Manage Default and Custom QoS Rules

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

Add a Custom QoS Rule for a Service or Application

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

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.
5. Make sure that the **Turn Internet Access QoS On** check box is selected.
6. Make sure that the **QoS By Service** radio button is selected.
7. From the **Applications** menu, select **Add a new application**.
   The page adjusts.
8. Specify a new QoS rule for a service or application as described in the following table.

Field	Description
Priority	
QoS Policy for	Enter a name for the QoS rule.
Priority	Select the priority (**Highest**, **High**, **Normal**, or **Low**) that must be assigned to the service or application. The priority selections correspond to the queue columns in the QoS rules table.

(Continued)

Field	Description
Specified Port Range	
Connection Type	Select the protocol (**TCP** or **UDP**) that is associated with the service or application. If you are unsure, select **TCP/UDP**.
Starting Port	Enter the start port number for the service or application.
Ending Port	Enter the end port number for the service or application.

9. On the QoS - Priority Rules page, click the **Apply** button.
   The new QoS rule is added to the QoS rules table.
10. On the QoS Setup page, click the **Apply** button.
    Your settings are saved.

Add a Custom QoS Rule for a Device

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

To add a QoS rule for a device:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.
5. Make sure that the **Turn Internet Access QoS On** check box is selected.
6. Select the **By Device** radio button.
   The page adjusts.

7. Either select the radio button for a device in the MAC Device List to complete the fields automatically (by default, each device is assigned a normal priority) or specify the settings for the device as described in the following table.

Field	Description
QoS Policy for	Enter a name for the QoS rule.
MAC Address	Enter the MAC address for the device.
Device	Enter the name of the device.
Priority	Select the priority (**Highest**, **High**, **Normal**, or **Low**) that must be assigned to the service or application. The priority selections correspond to the queue columns in the QoS rules table.

8. Click the **Add** button.
   The new QoS rule is added to the QoS rules table.
9. Click the **Apply** button.
   Your settings are saved.

Change a QoS Rule or Change the Priority for a Rule

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

To change a QoS 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 BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.
5. Make sure that the **Turn Internet Access QoS On** check box is selected.
6. In the QoS rules table, click the service, application, or device to select it.

The **Edit** button becomes available.

7. Click the **Edit** button.
   The QoS Priority Rules page displays.
8. Change the settings.
   For more information about the settings, see Add a Custom QoS Rule for a Service or Application on page 46 or Add a Custom QoS Rule for a Device on page 47.
9. On the QoS - Priority Rules page, click the **Apply** button.
   Your settings are saved. If you changed the priority, the QoS rule now displays in a different column of the QoS rules table on the QoS Setup page.

Remove a QoS Rule

You can remove an individual custom or default QoS rule.

To remove a QoS rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.
5. In the QoS rules table, click the service, application, or device to select it.
   The **Delete** button becomes available.
6. Click the **Delete** button.
   The QoS rule is removed.
7. Click the **Apply** button.
   Your settings are saved.

Remove All QoS Rules

You can permanently remove all custom and default QoS rules.

WARNING: If you remove all QoS rules, both the custom and default QoS rules are permanently removed. The only way to get the default QoS rules back is by returning the router to factory default settings.

To remove all QoS 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 BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.

   WARNING: If you click the **Delete All** button, all default and custom QoS rules are permanently removed.

5. Click the **Delete All** button.
   All QoS rules are permanently removed.
6. Click the **Apply** button.
   Your settings are saved.

Manage Uplink Bandwidth Control

Uplink bandwidth control lets you check the maximum uplink bandwidth that your Internet connection can support and specify the maximum uplink bandwidth.

To specify the maximum uplink bandwidth:

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

A login window opens.

3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.
5. To find out what uplink bandwidth your Internet connection supports, click the **Speedtest** button.
   The speed test checks your uplink bandwidth and the supported uplink bandwidth displays.
6. In the **Uplink bandwidth Maximum** field, enter the maximum uplink bandwidth that you want to specify.
7. From the associated menu, select **Kbps** or **Mbps**.
8. Click the **Apply** button.
   Your settings are saved.

Manage Wi-Fi Multimedia Quality of Service

Wi-Fi Multimedia Quality of Service (WMM QoS) prioritizes WiFi voice and video traffic over the WiFi link.

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

WMM QoS is automatically enabled for the router. In some circumstances you might want to disable WMM.

To manage WMM QoS:

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

3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
   The QoS Setup page displays.
5. Disable or enable WMM QoS by doing the following:
   - To disable WMM QoS for the 2.4 GHz radio, clear the **Enable WMM (Wi-Fi multimedia) settings (2.4GHz b/g/n)** check box.
   - To enable WMM QoS for the 2.4 GHz radio, select the **Enable WMM (Wi-Fi multimedia) settings (2.4GHz b/g/n)** check box.
     By default, WMM QoS is enabled for the 2.4 GHz radio.
   - To disable WMM QoS for the 5 GHz radio, clear the **Enable WMM (Wi-Fi multimedia) settings (5GHz a/n)** check box.
   - To enable WMM QoS for the 5 GHz radio, select the **Enable WMM (Wi-Fi multimedia) settings (5GHz a/n)** check box.
     By default, WMM QoS is enabled for the 5 GHz radio.
6. Click the **Apply** button.
   Your settings are saved.

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, enable UPnP.

To enable Universal Plug and Play:

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

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

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > UPnP**.
   The UPnP page displays.
5. Select the **Turn UPnP On** check box.
   By default, this check box is selected. UPnP for automatic device configuration can be enabled or disabled. If the **Turn UPnP On** check box is cleared, 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.

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

5

Manage the Basic WiFi Network Settings

This chapter describes how you can manage the basic WiFi network settings of the router.

The chapter includes the following sections:

Manage the Basic WiFi Settings and WiFi Security of the Main Network

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. The preset SSID and password are uniquely generated for every device to protect and maximize your WiFi security. You can find the preset SSID and password on the router label.

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

View or Change the Basic WiFi Settings and WiFi Security Settings

You can view or change the basic WiFi settings and WiFi security. The router is a dual-band WiFi access point that simultaneously supports the 2.4 GHz band for 802.11b/g/n devices and the 5 GHz band for 802.11a/n/ac devices.

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

To view or change the basic WiFi settings and WiFi security 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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **Wireless**.
   The Wireless Network page displays.
5. View or change the basic WiFi settings and security settings.
   The following table describes the fields on the Wireless Network page.

Field	Description
Region Selection	
Region	From the menu, select the region in which the router operates. **Note:** It might not be legal to operate the router in a region other than the regions listed in the menu. If your country or region is not listed, check with your local government agency.
Wireless Network (2.4GHz b/g/n)	
Name (SSID)	The SSID is the 2.4 GHz WiFi network name. If you did not change the SSID, the default SSID displays. The default SSID is also printed on the router label. **Note:** If you change the SSID, enter a 32-character (maximum), case-sensitive name in this field.
Channel	From the **Channel** menu, select **Auto** for automatic channel selection or select an individual channel. The default selection is Auto. **Note:** 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 situation occurs, experiment with different channels to see which is the best. **Note:** If you use multiple WiFi access points (APs), reduce interference by selecting different channels for adjacent APs. We recommend a channel spacing of four channels between adjacent APs (for example, use Channels 1 and 5, or 6 and 10).

(Continued)

Field	Description
Mode	From the **Mode** menu, select one of the following modes: • **Up to 54 Mbps**. Legacy mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11n devices to functioning at up to 54 Mbps. • **Up to 145 Mbps**. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11n devices to functioning at up to 145 Mbps. • **Up to 300 Mbps**. Performance mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11n devices to function at up to 300 Mbps. This mode is the default mode. **Note:** WPA-PSK security supports speeds of up to 54 Mbps. Even if your devices are capable of a higher speed, WPA-PSK security limits their speed to 54 Mbps.
Enable SSID Broadcast	By default, the router broadcasts its SSID so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast, clear the **Enable SSID Broadcast** check box. Turning off the SSID broadcast provides additional WiFi security, but users must know the SSID to be able to join the WiFi network of the router.
Enable 20/40 MHz Coexistence	By default, 20/40 MHz coexistence is enabled to prevent interference between WiFi networks in your environment at the expense of the WiFi speed. If no other WiFi networks are present in your environment, you can clear the **Enable 20/40 MHz Coexistence** check box to increase the WiFi speed to the maximum supported speed.

(Continued)

Field	Description
Security Options This information applies to the 2.4 GHz WiFi network.	
If you change the WiFi security, select one of the following WiFi security options for the router's WiFi network: • **None**. An open WiFi network that does not provide any security. Any WiFi device can join the WiFi network. We recommend that you do *not* use an open WiFi network. • **WEP**. Wired Equivalent Privacy (WEP) security is a legacy authentication and data encryption mode that is superseded by WPA-PSK and WPA2-PSK. The WEP option displays only if you select **Up to 54 Mbps** from the **Mode** menu. • **WPA2-PSK [AES]**. This option is the default setting. This type of security enables WiFi devices that support WPA2 to join the router's 2.4 GHz WiFi network. If you did not change the passphrase, the default passphrase displays. The default passphrase is printed on the router label. WPA2 provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select WPA-PSK [TKIP] + WPA2-PSK [AES] security. If you change the passphrase, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the router's WiFi network, a user must enter this passphrase. • **WPA-PSK [TKIP] + WPA2-PSK [AES]**. This type of security enables WiFi devices that support either WPA or WPA2 to join the router's 2.4 GHz WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps. To use this type of security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the router's WiFi network, a user must enter this passphrase. • **WPA/WPA2 Enterprise**. This type of security requires that your WiFi network can access a RADIUS server.	
Wireless Network (5GHz a/n/ac)	
Name (SSID)	The SSID is the 5 GHz WiFi band name. If you did not change the SSID, the default SSID displays. The default SSID is also printed on the router label. **Note:** If you change the SSID, enter a 32-character (maximum), case-sensitive name in this field.

(Continued)

Field	Description
Channel	From the **Channel** menu, select an individual channel for a 5 GHz SSID. The default channel depends on your selection from the **Region** menu. **Note:** 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 situation occurs, experiment with different channels to see which is the best. **Note:** If you use multiple WiFi access points (APs), reduce interference by selecting different channels for adjacent APs. We recommend a channel spacing of four channels between adjacent APs.
Mode	From the appropriate **Mode** menu, select one of the following modes for a 5 GHz SSID: • **Up to 289 Mbps**. Legacy mode. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network but limits 802.11ac and 802.11n devices to functioning at up to 289 Mbps. • **Up to 600 Mbps**. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network but limits 802.11ac devices to functioning at up to 600 Mbps. • **Up to 1300 Mbps**. Performance mode. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the selected WiFi network in the 5 GHz band of the network and allows 802.11ac devices to function at up to 1300 Mbps. This mode is the default mode.
Enable SSID Broadcast	By default, for an SSID in the 5 GHz band, the router broadcasts the SSID so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off an SSID broadcast, clear the appropriate **Enable SSID Broadcast** check box. Turning off an SSID broadcast provides additional WiFi security, but users must know the SSID to be able to join the WiFi network of the router.

(Continued)

Field	Description
Security Options This information applies to the 5 GHz WiFi network.	

If you change the WiFi security, select one of the following WiFi security options for the router's WiFi network:

- **None**. An open WiFi network that does not provide any security. Any WiFi device can join the selected WiFi network in the 5 GHz band of the WiFi network. We recommend that you do *not* use an open WiFi network.
- **WPA2-PSK [AES]**. This option is the default setting. This type of security enables WiFi devices that support WPA2 to join the selected WiFi network in the 5 GHz band of the WiFi network. If you did not change the passphrase, the default passphrase displays. The default passphrase is printed on the router label. WPA2 provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select WPA-PSK [TKIP] + WPA2-PSK [AES] security.
  If you change the passphrase, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the selected WiFi network in the 5 GHz band of the WiFi network, a user must enter this passphrase.
- **WPA-PSK [TKIP] + WPA2-PSK [AES]**. This type of security enables WiFi devices that support either WPA or WPA2 to join the selected WiFi network in the 5 GHz band of the WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps.
  To use this type of security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the selected WiFi network in the 5 GHz band of the WiFi network, a user must enter this passphrase.
- **WPA/WPA2 Enterprise**. This type of security requires that your WiFi network can access a RADIUS server.

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

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

7. Make sure that you can reconnect over WiFi to the network with its new settings.
   If you cannot connect over WiFi, check the following:

   - If your computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the router provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
   - If your computer or mobile device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your computer or mobile device to match the current settings for your network.
   - Does your computer or mobile device display as an attached device? (See View devices currently on the network on page 147.) If it does, it is connected to the network.

- Are you using the correct network name (SSID) and password?

Configure WEP Legacy WiFi Security

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

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

To configure WEP security:

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

   Note: If you are configuring a guest network, select **Guest Network** instead. The Guest Network Settings page displays. In this situtation disregardStep 5 and go toStep 6.

5. From the **Mode** menu, select **Up to 54 Mbps**.
   The page adjusts to display the **WEP** radio button.

   Note: If you are configuring a guest network, disregard this step.

6. In the Security Options section, select the **WEP** radio button.
7. From the **Authentication Type** menu, select one of the following types:
   - **Automatic**. Clients can use either Open System or Shared Key authentication.
   - **Shared Key**. Clients can use only Shared Key authentication.
8. From the **Encryption Strength** menu, select the encryption key size:

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

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

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

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

12. Make sure that you can reconnect over WiFi to the network with its new security settings.
    If you cannot connect over WiFi, check the following:
    - If your computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the router provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
    - If your computer or mobile device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your computer or mobile device to match the current settings for your network.
    - Does your computer or mobile device display as an attached device? (See View devices currently on the network on page 147.) If it does, it is connected to the network.
    - Are you using the correct WiFi network name (SSID) and password?

Configure WPA/WPA2 Enterprise WiFi Security

Remote Authentication Dial In User Service (RADIUS) is an enterprise-level method for centralized Authentication, Authorization, and Accounting (AAA) management. To enable the router to provide WPA and WPA2 enterprise WiFi security, the WiFi network that the router provides must be able to access a RADIUS server.

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

To configure WPA and WPA2 enterprise security:

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

   Note: If you are configuring a guest network, select **Guest Network** instead. The Guest Network Settings page displays.

5. In the Security Options section below either the Wireless Network (2.4GHz b/g/n) section or the Wireless Network (5GHz a/n/ac) section, select the **WPA/WPA2 Enterprise** radio button.
6. In the WPA/WPA2 Enterprise section, enter the settings as described in the following table.

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

(Continued)

Field	Description
RADIUS server Port	Enter the number of the port on the router that is used to access the RADIUS server for authentication. The default port number is 1812.
RADIUS server Shared Secret	Enter the shared secret (RADIUS password) that is used between the router and the RADIUS server during authentication of a WiFi user.

7. Click the **Apply** button.
   Your settings are saved.
8. Make sure that you can reconnect over WiFi to the network with its new security settings.
   If you cannot connect over WiFi, check the following:
   - If your computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the router provides. Some mobile devices automatically connect to the first open network without WiFi security that they discover.
   - If your computer or mobile device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your computer or mobile device to match the current settings for your network.
   - Does your computer or mobile device display as an attached device? (See View devices currently on the network on page 147.) If it does, it is connected to the network.
   - Are you using the correct network name (SSID) and password?

Use WPS to Add a Device to the WiFi Network

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

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

WPS supports WPA and WPA2 WiFi security. If your router network is open (no WiFi security is set, which is not the default setting for the router), connecting with WPS

automatically sets WPA + WPA2 WiFi security on the router network and generates a random passphrase. You can view this passphrase (see Manage the Basic WiFi Settings and WiFi Security of the Main Network on page 55).

Use WPS With the Push Button Method

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

To let a WiFi device join the router's main WiFi network using WPS with the push button method:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > WPS Wizard**.
   The page displays a description of the WPS method.
5. Click the **Next** button.
   By default, the **Push Button (recommended)** radio button is selected.
6. Either click the button onscreen or press the **WPS** button on the right side panel of the router.
   For two minutes, the router attempts to find the WiFi device (that is, the client) that you want to join the router's main WiFi network.
   During this time, the WiFi LED on the top panel of the router blinks.
7. Within two minutes, go to the WiFi device and press its **WPS** button to join the router's main WiFi network without entering a password.
   After the router establishes a WPS connection, the WiFi LED lights a solid color and the Add WPS Client page displays a confirmation message.
8. To verify that the WiFi device is connected to the router's main WiFi network, select **BASIC > Attached Devices**.
   The WiFi device displays onscreen.

Use WPS With the PIN Method

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

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > WPS Wizard**.
   The page displays a description of the WPS method.
5. Click the **Next** button.
   The Add WPS Client page adjusts.
   The **Push Button (recommended)** radio button is selected by default.
6. Select the **PIN Number** radio button.
7. In the **Enter Clients' PIN** field, enter the PIN number of the WiFi device.
8. Click the **Next** button.
   For four minutes, the router attempts to find the WiFi device (that is, the client) that you want to join the router's main WiFi network.
   During this time, the WiFi LED on the top panel of the router blinks.
9. Within four minutes, go to the WiFi device and use its WPS software to join the network without entering a password.
   After the router establishes a WPS connection, the WiFi LED lights a solid color and the Add WPS Client page displays a confirmation message.
10. To verify that the WiFi device is connected to the router's main WiFi network, select **BASIC > Attached Devices**.
    The WiFi device displays on the page.

Manage the Basic WiFi Settings and WiFi Security of the Guest Network

A guest network allows visitors to use the Internet without using your WiFi security password or with a different WiFi password. By default, the guest WiFi network is disabled. You can enable and configure the guest WiFi network for each WiFi band. The router simultaneously supports the 2.4 GHz band for 802.11n, 802.11g, and 802.11b devices and the 5 GHz band for 802.11ac, 802.11n, and 802.11a devices.

The WiFi mode of the guest WiFi network depends on the WiFi mode of the main WiFi network. For example, if you configure the WiFi mode for the main WiFi network as Up to 54 Mbps in the 2.4 GHz band, the guest WiFi network also functions in the Up to 54 Mbps mode in the 2.4 GHz band. For information about configuring the WiFi mode, see View or Change the Basic WiFi Settings and WiFi Security Settings on page 55. The channel also depends on the channel selection of the main WiFi network.

The router provides two default guest networks with the following names (SSIDs):

- **2.4 GHz band**. NETGEAR_Guest
- **5 GHz band**. NETGEAR-5G_Guest

By default, these networks are configured as open networks without security but are disabled. You can enable one or both networks. You can also change the SSIDs for these networks.

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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **Guest Network**.
5. Enable the guest network and configure its WiFi settings as described in the following table.

Field	Description
Wireless Network (2.4GHz b/g/n)	
Name (SSID)	The SSID is the 2.4 GHz WiFi band name. If you did not change the SSID, the default SSID displays, which is NETGEAR_Guest. To change the SSID in the 2.4 GHz WiFi band for the guest WiFi network, enter a 32-character (maximum), case-sensitive name in this field.
Enable Guest Network	By default, the guest WiFi network is disabled. To enable the guest WiFi network for the 2.4 GHz WiFi band, select the **Enable Guest Network** check box.
Enable SSID Broadcast	By default, the router broadcasts the SSID of the 2.4 GHz WiFi band so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast for the 2.4 GHz WiFi band for the guest WiFi network, clear the **Enable SSID Broadcast** check box.
Allow guests to see each other and access my local network	By default, WiFi clients that are connected to the 2.4 GHz WiFi band of the guest WiFi network cannot access WiFi devices or Ethernet devices that are connected to the main WiFi network. To allow access to the main WiFi network, select the **Allow guests to see each other and access my local network** check box.
Security Options	

If you want to change the WiFi security, select one of the following WiFi security options for the 2.4 GHz band of the guest WiFi network:

- **None**. An open WiFi network that does not provide any security. Any WiFi device can join the 2.4 GHz band of the guest WiFi network. This is the default setting for the guest WiFi network.
- **WEP**. Wired Equivalent Privacy (WEP) security is a legacy authentication and data encryption mode that is superseded by WPA-PSK and WPA2-PSK. The **WEP** option displays only if you configure the WiFi mode for the main WiFi network as Up to 54 Mbps in the 2.4 GHz band (see View or Change the Basic WiFi Settings and WiFi Security Settings on page 55).
- **WPA2-PSK [AES]**. WPA2 provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. Select WPA2-PSK [AES] security to allow 802.11n devices to connect to the 2.4 GHz band of the guest WiFi network at the fastest speed. If your network includes older devices that do not support WPA2, select WPA-PSK [TKIP] + WPA2-PSK [AES] security.
  To use WPA2 security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 2.4 GHz band of the guest WiFi network, a user must enter this passphrase.
- **WPA-PSK [TKIP] + WPA2-PSK [AES]**. This type of security enables WiFi devices that support either WPA or WPA2 to join the 2.4 GHz band of the guest WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps.
  To use WPA + WPA2 security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 2.4 GHz band of the guest WiFi network, a user must enter this passphrase.

(Continued)

Field	Description
Passphrase	The passphrase that provides users access to the guest WiFi network in the 2.4 GHZ band. The passphrase is also referred to as the *password* or *key*.
Wireless Network (5GHz a/n/ac)	
Name (SSID)	The SSID is the 5 GHz WiFi band name. If you did not change the SSID, the default SSID displays, which is NETGEAR-5G_Guest. To change the SSID in the 5 GHz WiFi band for the guest WiFi network, enter a 32-character (maximum), case-sensitive name in this field.
Enable Guest Network	By default, the guest WiFi network is disabled. To enable the guest WiFi network for an SSID in the 5 GHz WiFi band, select the appropriate **Enable Guest Network** check box.
Enable SSID Broadcast	By default, for an SSID in the 5 GHz band, the router broadcasts the SSID so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off an SSID broadcast for the 5 GHz WiFi band for the guest WiFi network, clear the appropriate **Enable SSID Broadcast** check box.
Allow guests to see each other and access my local network	By default, WiFi clients that are connected to an SSID in the 5 GHz WiFi band of the guest WiFi network cannot access WiFi devices or Ethernet devices that are connected to the main WiFi network. To allow access to the main WiFi network, select the appropriate **Allow guests to see each other and access my local network** check box.

(Continued)

Field	Description
Security Options	
If you want to change the WiFi security for an SSID in the 5 GHz band, select one of the following WiFi security options for that SSID in the guest WiFi network: • **None**. An open WiFi network that does not provide any security. Any WiFi device can join the selected WiFi network in the 5 GHz band of the guest WiFi network. This is the default setting for the guest WiFi network. • **WPA2-PSK [AES]**. WPA2 provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. Select WPA2-PSK [AES] security to allow 802.11ac and 802.11n devices to connect to the selected WiFi network in the 5 GHz band of the guest WiFi network at the fastest speed. If your network includes older devices that do not support WPA2, select WPA-PSK [TKIP] + WPA2-PSK [AES] security. To use WPA2 security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the WiFi network in the 5 GHz band of the guest WiFi network, a user must enter this passphrase. • **WPA-PSK [TKIP] + WPA2-PSK [AES]**. This type of security enables WiFi devices that support either WPA or WPA2 to join the selected WiFi network in the 5 GHz band of the guest WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps. To use WPA + WPA2 security, in the **Passphrase** field, enter a phrase of 8 to 63 characters. To join the 5 GHz band of the guest WiFi network, a user must enter this passphrase.	
Passphrase	The passphrase that provides users access to the selected WiFi network in the 5 GHz band of the guest WiFi network. The passphrase is also referred to as the *password* or *key*.

6. Click the **Apply** button.
   Your settings are saved.
7. Make sure that you can reconnect over WiFi to the guest network.
   If you cannot connect over WiFi, check the following:
   - If your computer or mobile device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the router provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
   - Does your computer or mobile device display as an attached device? (See View devices currently on the network on page 147.) If it does, it is connected to the network.
   - Are you using the correct network name (SSID) and password?

Enable or Disable the WiFi Radios

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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.
   The Advanced Wireless Settings page displays.
5. Do one of the following in the Wireless Network (2.4GHz b/g/n) section or Wireless Network (5GHz a/n/ac), or both sections:
   - **Turn off the radios**. Clear the **Enable Wireless Router Radio** check box. The WiFi LED turns off.
   - **Turn on the radios**. Select the **Enable Wireless Router Radio** check box. The WiFi LED lights.
6. Click the **Apply** button.
   Your settings are saved.

6

Control Access to the Internet

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

This chapter includes the following sections:

Set Up Parental Controls

To set up Parental Controls, you must download the NETGEAR genie app on your mobile device. For more information about the NETGEAR genie app, visit NETGEAR.com/genie.

After you set up and enable Parental Controls, you can change the web filtering level for each device on the network through the network map page on the genie app.

To set up Parental Controls:

1. Connect your mobile device to your router's WiFi network.
2. Launch the app store on your mobile device and download the NETGEAR genie app.
3. Launch the NETGEAR genie app.
   The dashboard displays.
4. Tap **Parental Controls**.
   The Parental Controls page displays.
5. To log in to your OpenDNS account, tap the **LOGIN** button, enter your OpenDNS user name, and tap the **LOGIN** button.
   Parental Controls is automatically enabled.
6. To create an OpenDNS account, tap **CREATE ACCOUNT**, fill in the fields, tap the **SIGN UP** button.
   Your account is created and Parental Controls is automatically enabled.
   For more information about how to setup Parental Controls using the NETGEAR genie app, see the *genie Mobile App User Manual*, which is available at downloadcenter.netgear.com/.

Enable access control to allow or block access to the Internet

You can use access control to block or allow access to the Internet through your router.

To set up access 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 BASIC Home page displays.

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

   The Access Control page displays.

5. Select the **Turn on Access Control** check box.

   You must select this check box before you can specify an access rule and use the **Allow** and **Block** buttons. When this check box is cleared, all devices are allowed to connect, even if a device is in the blocked list.

6. Select an access rule:

   - **Allow all new devices to connect**. With this setting, a new device can access your network. You don't need to enter the its MAC address. This is the default setting. We recommend that you leave this radio button selected.
   - **Block all new devices from connecting**. With this setting, a new device cannot access your router's Internet connection, but can still access your router's local network. Before a device accesses your router's Internet connection, you must enter its MAC address for an Ethernet connection and its MAC address for a WiFi connection in the allowed list.

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

7. To view allowed or blocked devices that are not connected, click one of the following links:

   - **View list of allowed devices not currently connected to the network**
   - **View list of blocked devices not currently connected to the network**

   The list displays.

8. To allow the WiFi-enabled computer or mobile device you're currently using to continue to access the Internet, select the check box next to your computer or device, and click the **Allow** button.
9. Click the **Apply** button.

   Your settings are saved.

Enable and Manage Network Access Control

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

To set up network access control:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Security > Access Control**.
   The Access Control page displays.
5. Select the **Turn on Access Control** check box.
   You must select this check box before you can specify an access rule and use the **Allow** and **Block** buttons. When the **Turn on Access Control** check box is cleared, all devices are allowed to connect, even if a device is in the list of blocked devices.
6. Click the **Apply** button.
   Your settings are saved.
7. Select an access rule for new devices:
   - **Allow all new devices to connect**. With this setting, if you add a new device, it can access your network. You do not need to enter its MAC address on this page. We recommend that you leave this radio button selected.
   - **Block all new devices from connecting**. With this setting, if you add a new device, before it can access your network, you must enter its MAC address for an Ethernet connection and its MAC address for a WiFi connection in the allowed list. For more information, see Manage Network Access Control Lists on page 76.

   The access rule does not affect previously blocked or allowed devices. It applies only to devices joining your network in the future after you apply these settings.
8. To manage access for currently connected computers and devices, do the following:

- If you blocked all new devices from connecting, to allow the computer or device that you are currently using to continue to access the network, select the check box next to your computer or device in the table, and click the **Allow** button.
- To either continue to allow or to block other computers and devices that are currently connected, select the check box next to the computer or device in the table, and click either the **Allow** button or the **Block** button.

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

Manage Network Access Control Lists

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

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

Each network device owns a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the WiFi card or network interface device. If you cannot see the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses through the web pages of the router (see View devices currently on the network on page 147).

Add Devices to or Remove Them From the Allowed List If you set up an access list that blocks all new devices from accessing your network, you must specify which devices are allowed to access your network.

To add or remove devices that are allowed:

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

5. Click the **View list of allowed devices not currently connected to the network** link.

   The Access Control page displays.

   A table displays the detected device name, MAC address, and connection type of the devices that are not connected but allowed to access the network.

6. To add a device to the allowed list, do the following:
   a. Click the **Add** button.
      The Add Allowed Device page displays.
   b. Enter the MAC address and device name for the device that you want to allow.
   c. On the Add Allowed Device page, click the **Apply** button.
      The device is added to the allowed list on the Access Control page.

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

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

Add Devices to or Remove Them From the Blocked List

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

To add or remove devices that are blocked:

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

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

5. Click the **View list of blocked devices not currently connected to the network** link.

   The Access Control page displays.

   A table displays the detected device name, MAC address, and connection type of the devices that are not connected and are blocked from accessing the network.

6. To add a device to the blocked list, do the following:
   a. Click the **Add** button.
      The Add Blocked Device page displays.
   b. Enter the MAC address and device name for the device that you want to block.
   c. On the Add Blocked Device page, click the **Apply** button.
      The device is added to the blocked list on the Access Control page.

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

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

Use Keywords to Block Internet Sites

You can block keywords and domains (websites) to prevent certain types of HTTP traffic from accessing your network. By default, keyword blocking is disabled and no domains are blocked.

Set Up Blocking

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

To set up keyword and domain blocking:

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

3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Sites**.
   The Block Sites page displays.
5. Specify a keyword blocking option:
   - **Per Schedule**. Use keyword blocking according to a schedule that you set. For more information, see Set Up a Schedule for Keyword Blocking and Outbound Firewall Rules on page 86.
   - **Always**. Use keyword blocking continuously.
6. In the **Type keyword or domain name here** field, enter a keyword or domain.
   Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .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 or domain is added to the **Block sites containing these keywords or domain names** field (which is also referred to as the blocked list).
8. To add more keywords or domains, repeatStep 6 andStep 7.
   The keyword list supports up to 32 entries.
9. Click the **Apply** button.
   Your settings are saved.

Remove a Keyword or Domain From the Blocked List

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

To remove a keyword or domain from the blocked list:

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

A login window opens.

3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Sites**.
   The Block Sites page displays.
5. In the **Block sites containing these keywords or domain names** field, select the keyword or domain.
6. Click the **Delete Keyword** button.
   The keyword or domain is removed from the blocked list.
7. Click the **Apply** button.
   Your settings are saved.

Remove All Keywords and Domains From the Blocked List

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

To remove all keywords and domains from the blocked list:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Sites**.
   The Block Sites page displays.
5. Click the **Clear List** button.
   All keywords and domains are removed from the blocked list.
6. Click the **Apply** button.
   Your settings are saved.

Specify a Trusted Computer

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

To specify a trusted device:

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

Manage Simple Outbound Firewall Rules for Services and Applications

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 Use Keywords to Block Internet Sites on page 78. This type of blocking is another aspect of the outbound firewall.

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

Add an Outbound Firewall Rule

You can add an outbound firewall rule to prevent access to a specific service or application on the Internet.

To add an outbound firewall 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 BASIC Home page displays.
4. Select **ADVANCED > Security > Block Services**.
   The Block Services page displays.
5. In the Services Blocking section, specify how the router applies outbound rules:
   - **Per Schedule**. Use keyword blocking according to a schedule that you set. For more information, see Set Up a Schedule for Keyword Blocking and Outbound Firewall Rules on page 86.
   - **Always**. Use keyword blocking continuously.
6. Below the Service Table, click the **Add** button.
   The Block Services Setup page displays.
7. From the **Service Type** menu, select service or application to be covered by this rule.
   If the service or application does not display in the list, you can add it (see Add an Outbound Firewall Rule for a Custom Service or Application on page 83).

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

Add an Outbound Firewall Rule for a Custom Service or Application

The router lists many default services and applications that you can use in outbound rules. If the service or application is not predefined, you can specify a custom service or application in an outbound rule.

To add an outbound firewall rule for a custom service or application:

1. Find out which protocol and port number or range of numbers the service or application uses.
   You can usually find this information by contacting the publisher of the service or application or through online user or news groups.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.
   A login window opens.
4. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
5. Select **ADVANCED > Security > Block Services**.
   The Block Services page displays.
6. If this is the first time that you add an outbound firewall rule, in the Services Blocking section, specify how the router applies outbound rules:

- **Per Schedule**. Use keyword blocking according to a schedule that you set. For more information, see Set Up a Schedule for Keyword Blocking and Outbound Firewall Rules on page 86.
- **Always**. Use keyword blocking continuously.

7. Below the Service Table, click the **Add** button.
   The Block Services Setup page displays.
8. From the **Service Type** menu, select **User Defined**.
9. Specify a new outbound rule as described in the following table.

Field	Description
Protocol	Select the protocol (**TCP** or **UDP**) that is associated with the service or application. If you are unsure, select **TCP/UDP**.
Starting Port	Enter the start port for the service or application.
Ending Port	If the service or application uses a range of ports, enter the end port for the range. If the service or application uses a single port, repeat the port number that you entered in the **Starting Port** field.
Service Type/User Defined	Enter the name of the custom service or application.

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

Change an Outbound Firewall Rule

You can change an existing outbound firewall rule.

To change an outbound firewall 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 BASIC Home page displays.
4. Select **ADVANCED > Security > Block Services**.
   The Block Services page displays.
5. In the Service Table, select the radio button for the rule.
6. Click the **Edit** button.
   The Block Services Setup page displays.
7. Change the settings.
   For information about the settings, see Add an Outbound Firewall Rule for a Custom Service or Application on page 83.
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

You can remove an outbound firewall rule that you no longer need.

To remove an outbound firewall 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 BASIC Home page displays.

4. Select **ADVANCED > Security > Block Services**.
   The Block Services page displays.
5. In the Service Table, select the radio button for the rule.
6. Click the **Delete** button.
   The rule is removed from the Service Table.

Set Up a Schedule for Keyword Blocking and Outbound Firewall Rules

You can set up a schedule that you can apply to keyword blocking and outbound firewall rules.

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 Set Up Blocking on page 78), outbound firewall rules (see Manage Simple Outbound Firewall Rules for Services and Applications on page 81), 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 BASIC Home page displays.
4. Select **ADVANCED > Security > Schedule**.
   The Schedule page displays.

5. Set up the schedule for blocking:
   - **Days to Block**. Select the check box for each day that you want to block access or specify that blocking occurs on every day by selecting the **Every Day** check box.
     By default, the **Every Day** check box is selected.
   - **Time of Day to Block**. Select a start and end time for blocking in 24-hour format or select the **All Day** check box for 24-hour blocking.
     By default, the **All Day** check box is selected.
6. From the **Time Zone** menu, select your time zone.
7. If you live in an area that observes daylight saving time, select the **Automatically adjust for daylight savings time** check box.

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

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

Set up security event email notifications

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

To set up email notifications:

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

   The BASIC Home page displays.
4. Select **ADVANCED > Security > 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, type the email address to which logs and alerts are to be sent.

   This email address is also used for the From address. If this field is blank, log and alert messages are not sent.
7. In the **Your Outgoing Mail Server** field, enter the name of your ISP outgoing (SMTP) mail server (such as mail.myISP.com).

   You might be able to find this information in the configuration window of your email program. If you leave this field blank, log and alert messages are not sent.
8. In the **Outgoing Mail Server Port Number** field, enter a port number in the field.

   If you do not know the port number, leave the default port number.
9. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box, and do the following:
   a. In the **User Name** field, type the user name for the outgoing email server.
   b. In the **Password** field, type the password for the outgoing email server.
10. To send alerts when someone attempts to visit a blocked site, select the **Send Alerts Immediately** check box.

    Email alerts are sent immediately when someone attempts to visit a blocked site.
11. To send logs based on a schedule, specify these settings:
    a. From **Send logs according to this schedule** menu, select the schedule type.
    b. From the **Day** menu, select the day.
    c. From the **Time** menu, select the time, and select the **am** or **pm** radio button.
12. Click the **Apply** button.

    Your settings are saved.

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

7

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: You can use a USB port on the router to connect a USB storage device like a flash drive or hard drive. Do not connect a computer, USB modem, CD drive, or DVD drive to a USB port on the router.

The chapter contains the following sections:

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

USB device requirements

The router works with most USB-compliant external flash and hard drives. For the most up-to-date list of USB devices that the router supports, visit kb.netgear.com/app/answers/detail/a_id/18985/~/readyshare-usb-drives-compatibility-list.

Some USB external hard drives and flash drives require you to load the drivers onto the computer before the computer can access the USB storage device. Such USB storage devices do not work with the router.

The router supports the following file system types for full read/write access:

- FAT16
- FAT32
- NTFS
- NTFS with compression format enabled
- Ext2
- Ext3
- Ext4
- HFS
- HFS+

Connect a USB storage device to the router

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

To connect a USB device:

1. Insert your USB storage device into a USB port on the router.
2. If your USB storage device uses a power supply, connect it.

   You must use the power supply when you connect the USB storage device to the router.

   When you connect the USB storage device to the router USB port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers on your local area network (LAN).

Access a storage device connected to the router

From a 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.

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 opens.
4. In the **Server Address** field, enter **smb://readyshare**.
5. When prompted, select the **Guest** radio button.
   If you set up access control on the router and you allowed your Mac to access the network, select the **Registered User** radio button and enter **admin** for the name and router admin password for the password. For more information about access control, see Enable access control to allow or block access to the Internet on page 73.
6. Click the **Connect** 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.

Back up Windows-based computers with ReadySHARE Vault

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

The following operating systems support ReadySHARE Vault:

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

To back up your Windows-based computer:

1. Connect a USB HDD storage device to a USB port on the router.
2. If your USB storage device uses a power supply, connect it.
   You must use the power supply when you connect the USB storage device to the router.

   When you connect the USB storage device to the router's USB port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers on your local area network (LAN).
3. Download ReadySHARE Vault from netgear.com/readyshare and install it on each Windows-based computer.
4. Launch ReadySHARE Vault.
5. Use the dashboard or the **Backup** tab to set up and run your backup.

Back up Mac computers with Time Machine

You can use Time Machine to back up your Mac computers onto a USB hard drive that is connected to one of the router's USB ports. You can access the connected storage device from your Mac with a wired or WiFi connection to your router.

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

Set up a USB hard drive on a Mac

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

To format your USB hard disk drive and specify partitions:

1. Physically connect the USB HDD to your router.
2. If your USB HDD uses a power supply, connect it.
   You must use the power supply when you connect the USB HDD to the router.

   When you connect the USB HDD to the router's port, it might take up to two minutes before it is ready for sharing. By default, the USB HDD is available to all computers on your local area network (LAN).
3. On your Mac, go to **Spotlight** (or the magnifying glass) at the top right of the page and search for Disk Utility.
4. Open the Disk Utility, select your USB HDD, click the **Erase** tab, and click the **Erase** button.
5. Click the **Partition** tab.
6. In the **Partition Layout** menu, set the number of partitions that you want to use.
7. Click the **Options** button.
   The Partition schemes display.
8. Select the **GUID Partition Table** or **Master Boot Record** radio button.
9. In the **Format** menu, select **Mac OS Extended (Journaled)**.
10. Click the **OK** button.
11. Click the **Apply** button.
    Your settings are saved.

Prepare to back up a large amount of data

Before you back up a large amount of data with Time Machine, we recommend that you follow this procedure.

To prepare to back up a large amount of data:

1. Upgrade the operating system of the Mac computer.
2. Verify and repair the backup disk and the local disk.
3. Verify and repair the permissions on the local disk.
4. Set Energy Saver:
   a. From the **Apple** menu, select **System Preferences**.
   The System Preferences page displays.
   b. Select **Energy Saver**.
   The Energy Saver page displays.
   c. Click the **Power Adapter** tab.
   d. Select the **Wake for Wi-Fi network access** check box.
   e. Click the **back arrow** to save the changes and exit the page.
5. Modify your security settings:
   a. On the **System Preferences** page, select **Security & Privacy**.
   The Security & Privacy page displays.
   b. Click the **Advanced** button at the bottom of the page.
   If the **Advanced** button is grayed out, click the lock icon so that you can change the settings.
   c. Clear the **Log out after minutes of inactivity** check box.
   d. Click the **OK** button.
   Your settings are saved.

Use Time Machine to back up onto a USB hard disk

You can use Time Machine to back up your Mac computers onto a USB hard disk drive (HDD) that is connected to one of the router's USB ports.

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

1. Prepare your USB device with a compatible format and partitions.
   For more information, see Set up a USB hard drive on a Mac on page 94.
2. If you plan to back up a large amount of data, see Prepare to back up a large amount of data on page 95.

3. If your USB HDD uses a power supply, connect it.
   You must use the power supply when you connect the USB HDD to the router.
   When you connect the USB HDD to the router's port, it might take up to two minutes before it is ready for sharing. By default, the USB HDD is available to all computers on your local area network (LAN).
4. On a Mac computer that is connected to the network, launch Finder and select **Go > Connect to Server**.
   The Connect to Server window opens.
5. Type **smb://routerlogin.net** and click the **Connect** button.
6. When prompted, select the **Registered User** radio button.
7. Enter **admin** for the name and the router admin password for the password and click the **Connect** button.
   A list of USB devices connected to your router displays.
8. From the **Apple** menu, select **System Preferences**.
   The System Preferences window displays.
9. Select **Time Machine**.
   The Time Machine window displays.
10. Click the **Select Backup Disk** button and select your USB HDD from the list.
11. Click the **Use Disk** button.

    Note: If you do not see the USB partition that you want in the Time Machine disk list, go to Mac Finder and click that USB partition. It displays in the Time Machine list.

12. When prompted, select the **Registered User** radio button.
13. Enter **admin** for the name and the router admin password for the password and click the **Connect** button.

When the setup is complete, the Mac automatically schedules a full backup. You can back up immediately.

Manage Access to a Storage Device

You can specify the device name, workgroups, and network folders for a storage device connected to the USB port on the router.

To specify the storage device access settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > USB Storage > ReadySHARE**.
   The USB Storage (Advanced Settings) page displays.
5. To specify a name that is used to access the USB device or devices that are connected to the router, in the **Network/Device Name** field, enter a name.
   By default, the name is readyshare.
6. 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.
7. Enable or disable access methods by selecting or clearing the corresponding check boxes and specifying access to the storage device as described in the following table.

Access Method	Description
Network Connection	Enabled by default. You can type **\\readyshare** to access the storage device within your network. If you change the name in the **Network/Device Name** field from readyshare to another name, the link changes accordingly. You can enable password protection.
HTTP	Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB device within your network and download or upload files. In this URL, readyshare is the name that is specified in the **Network/Device Name** field. If you change the name in the **Network/Device Name** field from readyshare to another name, the link changes accordingly. You can also click the link that is shown in the Link column. The fixed port is number is 80. You can enable password protection.
HTTPS (via internet)	Disabled by default. If you enable this feature, remote users can type **https://***<public IP address>***/shares** to access the USB device over the Internet. *<public IP address>* is the external or public IP address that is assigned to the router (for example, 1.1.10.102). This feature supports file uploading only. The default port is number 443, which you can change. Password protection is enabled by default.
FTP	Enabled by default. You can type **ftp://readyshare.routerlogin.net/shares** to access the USB device within your network and download or upload files. In this URL, readyshare is the name that is specified in the **Network/Device Name** field. If you change the name in the **Network/Device Name** field from readyshare to another name, the link changes accordingly. You can also click the link that is shown in the Link column. The fixed port is number is 21. You can enable password protection.
FTP (via internet)	Disabled by default. If you enable this feature, remote users can type **ftp://***<public IP address>***/shares** to access the USB device over the Internet and download or upload files. *<public IP address>* is the external or public IP address that is assigned to the router (for example, 1.1.10.102). The default port is number 21, which you can change. Password protection is enabled by default. If you set up Dynamic DNS, you can also type a URL domain name. For example, if your domain name is MyName and you use the NETGEAR DDNS server, you can type **ftp://MyName.mynetgear.com** to access the USB device over the Internet and download or upload files.

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

Enable FTP access within your network

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

To enable 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 BASIC Home page displays.
4. Select **ADVANCED > USB Storage > ReadySHARE**.
   The USB Storage (Advanced Settings) page displays.
5. Select the **FTP** check box.
6. Click the **Apply** button.
   Your settings are saved.

View network folders on a storage device

You can view network folders on a storage device that is 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 BASIC Home page displays.
4. Select **ADVANCED > USB Storage > ReadySHARE**.

The USB Storage (Advanced Settings) page displays.

5. Scroll down to the Available Networks Folder section to view the following settings:
   - **Share Name**. If only one USB device is connected, the default share name is USB_Storage.
     You can click the name or you can type it in the address field of your web browser. If Not Shared is shown, the default share was deleted and no other share for the root folder exists.
   - **Read Access and Write Access**. 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**. 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 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 BASIC Home page displays.
4. Select **ADVANCED > USB Storage > ReadySHARE**.
   The USB Storage (Advanced Settings) page displays.
5. In the Available Network Folders section, select the USB storage device.
   If a single device is attached to the USB port, the radio button is selected automatically.

6. Click the **Create Network Folder** button.
   The Add 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. From the **USB Device** menu, select the USB drive.

   Note: We recommend that you do not attach more than one drive to one USB port (for example, through a USB hub).

8. Click the **Browse** button and in the Folder field, select the folder.
9. In the **Share Name** field, type the name of the share.
10. From the **Read Access** menu and the **Write Access** menu, select the settings that you want.
    All–no password (the default) allows all users to access the network folder. The other option is that only the admin user is allowed access to the network folder. The password for admin is the same one that you use to log in to the router.
11. Click the **Apply** button.
    The folder is added on the USB storage device.
12. Click the **Close Window** button.
    The window closes.

Edit a network folder on a USB storage device

You can edit network folders on a USB storage devices connected to a router USB port.

To edit 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 BASIC Home page displays.

4. Select **ADVANCED > USB Storage > ReadySHARE**.
   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.

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 BASIC Home page displays.
4. Select **ADVANCED > USB Storage > ReadySHARE**.
   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.
   This takes the device offline.
7. Physically disconnect the USB storage device.

8

Use Dynamic DNS to Access USB Storage Devices Through the Internet

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

This chapter contains 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 FTP Access Through the Internet

To set up FTP access:

1. Launch a web browser from a computer or moblile 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 BASIC Home page displays.
4. Select **ADVANCED > USB Storage > ReadySHARE**.
   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, select a device in the Available Network Folder's section.
   If only one device is connected, it is automatically selected.

8. Click the **Edit** button.
   The Edit page displays.
9. In the **Read Access** list, select **admin**.
10. In the **Write Access** list, select **admin**.
11. Click the **Apply** button.
    Your settings are saved.

Your personal FTP server

With your customized free URL, you can use FTP to access your network when you aren't home through Dynamic DNS. To set up your FTP server, you must register for a NETGEAR Dynamic DNS (DDNS) service account and specify the account settings. See Set up a new Dynamic DNS account on page 106.

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.

Set Up Your Personal FTP Server

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 106.
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 104.

6. On a remote computer with Internet access, you can use FTP to access your router using ftp://*yourname*.mynetgear.com.

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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.
   The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select **NETGEAR**.
   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. Click the **Register** button.
12. Follow the onscreen instructions 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.
   The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select your provider.
7. Select the **Yes** radio button.
   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. Depending on the type of service, specify either the user name of the email address:
   - **No-IP account or DynDNS account**. In the **User Name** field, type the user name for your account.
   - **NETGEAR account**. In the **Email** field, type the email address for your account.
10. In the **Password (6-32 characters)** field, type the password for your DDNS account.
11. Click the **Apply** button.
    Your settings are saved.
12. 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.
   The Dynamic DNS page displays.
5. Change your DDNS account settings as necessary.
6. Click the **Apply** button.
   Your settings are saved.

Access USB storage devices through the Internet

You can access USB storage devices through the Internet when you're not home.

To access 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 104.
   - To connect without Dynamic DNS, type the router's Internet port IP address.

   You can view the router's Internet IP address on the BASIC Home page.

You can use FTP to share files on a USB device connected to the router.

9

Use the Router as a Media Server

This chapter contains the following sections:

Specify ReadyDLNA Media Server Settings

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

To specify media server settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > USB Storage > ReadySHARE > Media Server**.
   The Media Server (Settings) page displays.
5. Specify the settings:
   - **Enable DLNA Media Server**. Select this check box to enable this device to act as a media server.
   - **Enable TiVo support**. Select this check box if you want to play ReadyNAS media on your TiVo device. For more information, see Set Up the Router to Work With TiVo on page 113.
   - **Enable iTunes Server (Music Only)**. Select this check box if you want to play music from a USB device that is connected to your router with iTunes on your Windows-based or Mac computer using Home Sharing. For more information, see Set Up the Router's iTunes Server With iTunes on page 111.
   - **Media Server Device Name**. Click the **Edit** button to change the router's media server name.

     Note: If you change the media server name, you can also change the ReadySHARE storage folder access path to the new name or keep the access path as `\\readyshare .`

   - **Content Scan**. The router automatically scans for media files whenever new files are added to your ReadySHARE USB storage device. Only a shared folder with

All – no password in **Read Access** can be scanned for media files. To scan for new media files immediately, click the **Rescan media files** button.

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

Play Music From a Storage Device With iTunes Server

iTunes server lets you play music from a USB device that is connected to a USB port on your router with iTunes on your Windows-based or Mac computer or with the Apple Remote app on your iPhone or iPad. You can also use the Apple Remote app from an iPhone or iPad to play music on any AirPlay devices, such as Apple TV or AirPlay-supported receivers.

Supported music file formats are MP3, AAC, and FLAC. The maximum number of music files supported is 10,000.

Set Up the Router's iTunes Server With iTunes

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

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

1. Connect a USB storage device to a USB port on your router.
2. If your USB storage device uses a power supply, connect it.
   You must use the power supply when you connect the USB storage device to the router.

   When you connect the USB storage device to the router's USB port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers on your local area network (LAN).
3. Launch a web browser from a computer or mobile device that is connected to the router network.
4. Enter **http://www.routerlogin.net**.
   A login window opens.
5. Enter the router admin user name and password.

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

The BASIC Home page displays.

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

Set Up the Router's iTunes Server With the Remote App

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

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

1. Connect a USB storage device to a USB port on your router.
2. If your USB storage device uses a power supply, connect it.
   You must use the power supply when you connect the USB storage device to the router.

   When you connect the USB storage device to the router's USB port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers on your local area network (LAN).
3. Connect your iPhone or iPad to your router's WiFi network.
4. Download the Remote app from the Apple App Store.
5. Launch the Remote app from your iPhone or iPad.
6. In the Remote app, click the **Add a Device** button.

The passcode displays in the Remote app.

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

Set Up the Router to Work With TiVo

You can set up your TiVo to access media files stored on a USB device that is connected to your router. The TiVo must be on the same network as the router. This feature supports the following file formats:

- **Video**. See and play `mpeg1`, and `mpeg2` files.
- **Music**. See and play MP3 files.
- **Pictures**. View images in `.jpg` format.

You can use the TiVo (Series 2 and later) Home Media Option to play photos and music on your Windows or Mac computer in your TiVo user interface.

To set up the router to work with TiVo:

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

10

Manage the WAN and LAN Network Settings

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

The chapter includes the following sections:

Change the WiFi Mbps Settings

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

To change the WiFi Mbps settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **Wireless**.
   The Wireless Settings page displays.
5. For the 2.4 GHz WiFi band, in the Wireless Network (2.4 GHz b/g/n) section, select a setting from the **Mode** menu.
6. For the 5 GHz WiFi band, select a setting from the **Mode** menu.
7. Click the **Apply** button.
   Your settings are saved.

Manage the WAN Security Settings

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

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

To change the default WAN security settings:

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

A login window opens.

3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. To enable a port scan and disable DoS protection, select the **Disable Port Scan and DoS Protection** check box.
6. To enable the router to respond to a ping, select the **Respond to Ping on Internet Port** check box.
7. Click the **Apply** button.
   Your settings are saved.

Set up a default DMZ server

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

Manage 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. If you do not need this feature, leave it disabled, which is the default setting.

To enable IGMP proxying:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. Clear the **Disable IGMP Proxying** check box.
   By default, the **Disable IGMP Proxying** check box is selected and IGMP proxying is disabled.
6. Click the **Apply** button.

Your settings are saved.

Manage VPN Pass-Through

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

To disable VPN pass-through:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. In the VPN Passthrough section, select one or more **Disabled** radio buttons.
   By default, the **Enabled** radio buttons are selected and VPN pass-through is enabled for IPSec, PPTP, and L2TP.
6. Click the **Apply** button.
   Your settings are saved.

Manage 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. Secured NAT is the default setting.

To change the default NAT filtering settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. Select a NAT Filtering radio button:
   - **Secured**. Provides a secured firewall to protect the computers on the LAN from attacks from the Internet but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. By default, the **Secured** radio button is selected.
   - **Open**. Provides a much less secured firewall but allows almost all Internet applications to function.
6. Click the **Apply** button.
   Your settings are saved.

Manage the SIP Application-Level Gateway

The application-level gateway (ALG) for the Session Initiation Protocol (SIP) is enabled by default for enhanced address and port translation. However, some types of VoIP and video traffic might not work well when the SIP ALG is enabled. For this reason, the router provides the option to disable the SIP ALG.

To change the default SIP ALG setting:

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

3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
   The WAN Setup page displays.
5. To disable the SIP ALG, select the **Disable SIP ALG** check box.
   The SIP ALG is enabled by default.
6. Click the **Apply** button.
   Your settings are saved.

Manage the LAN IP Address Settings

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

- **LAN IP address**. 192.168.1.1 (this is the same as www.routerlogin.net)
- **Subnet mask**. 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. The IP address and subnet mask identify which addresses are local to a specific device and which must be reached through a gateway or router. 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 competing subnets use the same IP scheme.

To change the LAN IP address 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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.

The LAN Setup page displays.

5. In the **IP Address** fields, enter the LAN IP address for the router.
6. In the **IP Subnet Mask** fields, enter the LAN subnet mask for the router.
7. Click the **Apply** button.

   Your settings are saved.

   If you changed the LAN IP address of the router, you are disconnected when the changes take effect.

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

Manage the Router Information Protocol Settings

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

To manage the RIP settings:

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

   A login window opens.

3. Enter the router user name and password.

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

   The BASIC Home page displays.

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

   The LAN Setup page displays.

5. From the **RIP Direction** menu, 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 but does not incorporate the RIP information that it receives.

- **In Only**. The router incorporates the RIP information that it receives but does not broadcast its routing table.

6. From the **RIP Version** menu, select the RIP version:
   - **Disabled**. The RIP version is disabled. This is the default setting.
   - **RIP-1**. This format is universally supported. It is adequate for most networks, unless you are using an unusual network setup.
   - **RIP-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.
7. Click the **Apply** button.
   Your settings are saved.

Manage the DHCP Server Address Pool

By default, the router acts as a Dynamic Host Configuration Protocol (DHCP) server. The router assigns IP, DNS server, and default gateway addresses to all computers that are connected to its LAN and WiFi network. 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. The default DHCP address pool is 192.168.1.2–192.168.1.254.

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)

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

4. Select **ADVANCED > Setup > LAN Setup**.
   The LAN Setup page displays.
5. Make sure that the **Use Router as DHCP Server** check box is selected.
   This check box is selected by default.
6. Specify the range of IP addresses that the router assigns:
   - In the **Starting IP Address** field, enter the lowest number in the range.
     This IP address must be in the same subnet as the router. By default, the starting IP address is 192.168.1.2.
   - In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.
     This IP address must be in the same subnet as the router. By default, the ending IP address is 192.168.1.254.
7. Click the **Apply** button.
   Your settings are saved.

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.

Edit a reserved IP address

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

5. Select the radio button next to the reserved address that you want to edit.
6. Click the **Edit** button.
   The Address Reservation page displays.
7. Change the settings.
8. 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 BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
   The LAN Setup page displays.
5. Select the radio button next to the reserved address that you want to delete.
6. Click the **Delete** button.
   The address is removed.

Disable the Built-In DHCP Server

By default, the router functions as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all devices 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.

Note: If you disable the DHCP server and no other DHCP server is available on your network, you must set your computer IP addresses manually so that they can access the router.

To disable the built-in 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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > 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.

Change the Router's Device Name

The router's default device name is its model number.

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

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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.

The LAN Setup page displays.

5. Type a new name in the **Device Name** field.
6. Click the **Apply** button.
   A pop-up window displays.
7. Click the **Yes** button.
   The router restarts.

Set Up and Manage Custom Static Routes

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

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

- Your primary Internet access is through an ADSL modem to an ISP.
- You use an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.
- Your company's network address is 134.177.0.0.

When you first configured 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 attempt 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 request is likely to be denied by the company's firewall.

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

- Through the destination IP address and IP subnet mask, specify that this static route applies to all 134.177.x.x addresses.
- Through the gateway IP address, specify that all traffic for these addresses is forwarded to the ISDN router at 192.168.1.100.

Set Up a Static Route

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

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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.
   The Static Routes page displays.
5. Click the **Add** button.
   The page adjusts.
6. To make the route private, select the **Private** check box.
   A private static route is not reported in RIP.
7. To prevent the route from becoming active after you click the **Apply** button, clear the **Active** check box.
   In some situations, you might want to set up a static route but keep it disabled until a later time. By default, the **Active** check box is selected and a route becomes active after you click the **Apply** button.
8. Enter the settings as described in the following table.

Field	Description
Destination IP Address	Enter the IP address for the final destination of the route.
IP Subnet Mask	Enter the IP subnet mask for the final destination of the route. If the destination is a single host, enter **255.255.255.255**.

(Continued)

Field	Description
Gateway IP Address	Enter the IP address of the gateway. The IP address of the gateway must be on the same LAN segment as the router.
Metric	Enter a number from 2 through 15. This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.

9. Click the **Apply** button.
   Your settings are saved. The static route is added to the table on the Static Routes page.

Change a Static Route

You can change an existing 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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.
   The Static Routes page displays.
5. In the Static Routes table, select the radio button for the route.
6. Click the **Edit** button.
   The page adjusts.
7. Change the settings for the route.
   For more information about the settings, see Set Up a Static Route on page 128.
8. Click the **Apply** button.
   The route is updated in the table on the Static Routes page.

Remove a Static Route

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

To remove 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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.
   The Static Routes page displays.
5. In the Static Routes table, select the radio button for the route.
6. Click the **Delete** button.
   The route is removed from the table on the Static Routes page.

Set Up a Bridge for 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 on how to set up a bridge for IPTV and Internet service, follow those instructions.

Set Up a Bridge for a Port Group

If the devices that are connected to the router's Ethernet LAN port or WiFi network include an IPTV device, your ISP might require you to set up a bridge for a port group for the router's Internet interface.

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

To configure a port group and enable the bridge:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.
   The VLAN / Bridge Settings page displays.
5. Select the **Enable VLAN Tag** check box.
   The page expands.
6. Select the **By bridge group** radio button.
   The page adjusts.
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 Devices 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 Devices 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 for a VLAN Tag Group

If the devices that are connected to the router's Ethernet LAN ports or WiFi network include an IPTV device, your ISP might require you to set up a bridge for a VLAN tag group for the router's Internet interface.

If you are subscribed to IPTV service, 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 IPTV 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 add a VLAN tag group and enable the bridge:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.
   The VLAN / Bridge Settings page displays.
5. Select the **Enable VLAN Tag** check box.
   The page expands.
6. Select the **By VLAN tag group** radio button.
   The page adjusts.
   The router includes a default VLAN tag group with the name Internet.
7. Click the **Add** button.
   The VLAN/IPTV Setup page displays.
8. Specify the settings as described in the following table.

Field	Description
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 tag group is added.
10. Click the **Apply** button.
    Your settings are saved.

11

Manage Your Router

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

The chapter contains the following sections:

Update the router firmware

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

Check for new firmware and update the router

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

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 that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > 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.

When the upload is complete, your router restarts. 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.

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` or `.chk` extension.

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

   The BASIC Home page displays.
5. Select **ADVANCED > Administration > Firmware Update**.
   The Firmware Update page displays.
6. Click the **Browse** button.
7. Find and select the firmware file on your computer.
8. Click the **Upload** button.
   The router begins the upload.

   Note: 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. Wait until the router finishes restarting. If your router does not reboot, check the Router Status page to confirm whether the new firmware version uploaded.

Change the admin password

The admin password is the one you specified the first time you logged in. You can change this password.

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

To change the password for the admin user 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 BASIC Home page displays.
4. Select **ADVANCED > Administration > Set Password**.
   The Set Password page displays.
5. Type the old password in the **Old Password** field.
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 so that 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 BASIC Home page displays.
4. Select **ADVANCED > 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 router 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 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 BASIC Home page displays.
4. Select **ADVANCED > 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 settings

To restore 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 BASIC Home page displays.

4. Select **ADVANCED > 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.

Disable or Enable LED Blinking or Turn Off LEDs

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

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

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

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > LED Control Settings**.
   The LED Control Settings page displays.

5. Select an LED control setting:
   - **Enable blinking on Internet LED, LAN LED, Wireless LED and USB LED when data traffic is detected**. Allows standard LED behavior. This setting is enabled by default.
   - **Disable blinking on Internet LED, LAN LED, Wireless LED and USB LED when data traffic is detected**. Blinking is disabled when data traffic is detected.
   - **Turn off all LEDs except Power LED**. All the LEDs, except the Power LED, are turned off.
6. Click the **Apply** button.
   Your settings are saved.

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.

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

CAUTION: This process erases all settings that you configured in the router.

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: To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, if you are connected to the router web interface, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting.

Erase the settings

CAUTION: This process erases all settings that you configured in the router.

To erase the 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 BASIC Home page displays.

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

   The Backup Settings page displays.

5. Click the **Erase** button.

   The configuration is reset to factory default settings. When the reset is complete, the router restarts. This process takes about two minutes.

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

View the Status and Statistics of the Router

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

View information about the router and the Internet and WiFi settings

You can view router information, the Internet port status, and WiFi settings.

To view information about the router and the Internet, modem, and 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 BASIC Home page displays.
4. Click the **ADVANCED** tab.
   The ADVANCED Home page displays.
   The information on this page uses the following color coding:
   - A green icon indicates that the Internet connection is fine and no problems exist. For a WiFi network, the network is enabled and secured.
   - A red icon indicates that configuration problems exist for the Internet connection or the connection is down. For a WiFi network, the network is disabled or down.
   - An amber icon indicates that the Internet port is configured but cannot get an Internet connection (for example, because the cable is disconnected), that a WiFi network is enabled but unprotected, or that another situation that requires your attention occurred.

Display the statistics of the Internet port

To display the statistics of the Internet port:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Click the **ADVANCED** tab.
   The ADVANCED Home page displays.
5. In the Internet Port pane, click the **Show Statistics** button.
   The Show Statistics window opens and displays following 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. For each port, the window displays the following information:
     - **Status**. The link status of the port.
     - **TxPkts**. The number of packets transmitted on this port since the router was last started.
     - **RxPkts**. The number of packets received on this port since the router was last started.
     - **Collisions**. The number of collisions on this port since the router was last started.
     - **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.
6. To change the polling frequency, enter a time in seconds in the **Poll Interval** field and click the **Set Interval** button.

To stop the polling entirely, click the **Stop** button.

Check the Internet connection status

To check the Internet connection status:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Click the **ADVANCED** tab.
   The ADVANCED Home page displays.
5. In the Internet Port pane, click the **Connection Status** button.
   The Connection Status window opens. The information that displays depends on the type of Internet connection.
   For example, if your Internet connection does not require a login and the router receives an IP address automatically, the window displays the following information:
   - **IP Address**. The IP address that is assigned to the router.
   - **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 lease was obtained.
   - **Lease Expires**. The date and time that the lease expires.
6. To release (stop) the Internet connection, click the **Release** button.
7. To renew (restart) the Internet connection, click the **Renew** button.
8. To exit the screen, click the **Close Window** button.

Manage the Activity Log

The log is a detailed record of the websites that users on your network accessed or attempted to access and many other router actions. Up to 256 entries are stored in the log. You can manage which activities are logged.

View, Email, or Clear the Logs

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

To view, email, or clear the 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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Logs**.
   The Logs page displays the following information:
   - **Action**. The action that occurred, such as whether Internet access was blocked or allowed.
   - **Source**. The name, IP address, or MAC address of the target device, application, or website for this log entry.
   - **Target**. The name, IP address, or MAC address of the target device, application, or website for this log entry.
   - **Date and Time**. The date and time at which the action occurred.
5. To refresh the log entries onscreen, click the **Refresh** button.
6. To clear the log entries, click the **Clear Log** button.
7. To email the log immediately, click the **Send Log** button.
   The router emails the logs to the address that you specified (see Set up security event email notifications on page 87).

Specify Which Activities Are Logged

You can specify which activities are logged. These activities display in the log and are forwarded to the syslog server if you enabled the syslog server function.

To manage which activities are logged:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Logs**.
   The Logs page displays.
5. Select the check boxes that correspond to the activities that you want to be logged.
   By default, all check boxes are selected.
6. Clear the check boxes that correspond to the activities that you do not want to be logged.
7. Click the **Apply** button.
   Your settings are saved.

View devices currently on the network

You can view all computers and devices that are currently connected to your network.

To view 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 BASIC Home page displays.

4. Select **Attached Devices**.
   The following information is displayed:
   - **Connection Type**. Wired or the WiFi band for the connection.
   - **Device Name**. If the device name is known, it is shown here.
   - **IP Address**. The IP address that the router assigned to this device when it joined the network. This address can change if a device is disconnected and rejoins the network.
   - **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label of the device.
5. To update this page, click the **Refresh** button.

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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.
   The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
   By default, no traffic limit is specified and the traffic volume 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 149.

View the Internet Traffic Volume and Statistics

If you enabled the traffic meter, 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 user name and password.

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

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.

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

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

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

   The Traffic Status pop-up window displays.

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 in 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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.
   The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
6. Select the **Traffic volume control by** radio button.
7. From the corresponding menu, select an option:
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
8. In the **Monthly Limit** field, enter how many MBytes (MB) per month are allowed.
9. If your ISP charges you for extra data volume when you make a new connection, enter the extra data volume in MB in the **Round up data volume for each connection by** field.
10. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
11. In the Traffic Control section, enter a value in 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 green**. This setting is optional. When the traffic limit is reached, the Internet LED blinks alternating green and amber.

- **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.

13. Click the **Apply** button.
    Your settings are saved and the router restarts.

    The Internet Traffic Statistics section helps you to monitor the data traffic.

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

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > 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 Traffic Control section, 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 green**. This setting is optional. When the traffic limit is reached, the Internet LED alternates blinking green and amber.
    - **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.
11. Click the **Apply** button.
    Your settings are saved and the router restarts.

    The Internet Traffic Statistics section helps you to monitor the data traffic.

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

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.
   The Traffic Meter page displays.
5. In the Traffic Control section, clear the **Disconnect and disable the Internet connection** check box.
6. Click the **Apply** button.
   Your settings are saved and the router restarts.

Remote access

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

Note: Be sure to change the password for the user name admin to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters. See Change the admin password on page 137.

Set up remote management

To set up remote management:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Remote Management**.
   The Remote Management page displays.
5. Select the **Turn Remote Management On** check box.
6. In the Allow Remote Access By section, specify the external IP addresses to be allowed to access the router's remote management.

   Note: For enhanced security, restrict access to as few external IP addresses as practical.

   Select one of the following:

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

- **Everyone**. Allow access from any IP address on the Internet.

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

Use remote access

To use remote access:

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

12

Manage the Advanced WiFi Features

This chapter describes how you can manage the advanced WiFi features of the router.

The chapter includes the following sections:

Set Up a WiFi Schedule

You can use this feature to 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. You can set up a separate WiFi schedule for each WiFi band.

To set up the WiFi schedule for a WiFi band:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.
   The Advanced Wireless Settings page displays.
5. In the Advanced Wireless Settings section for the 2.4 GHz band or the 5 GHz band, click the **Add a new period** button.
   The When to turn off wireless signal page displays.
6. Use the menus, radio buttons, and check boxes to set up a period during which you want to turn off the WiFi signal and specify whether the schedule is recurrent.
7. Click the **Apply** button.
   The Advanced Wireless Settings page displays.
8. Select the **Turn off wireless signal by schedule** check box to activate the schedule.
9. Click the **Apply** button.
   Your settings are saved.

Manage the WPS Settings

Wi-Fi Protected Setup (WPS) lets you join the WiFi network without typing the WiFi password. You can change the WPS default settings.

To manage WPS settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.
   The Advanced Wireless Settings page displays.
5. Scroll down to the WPS Settings section in the lower part of the page.
   The Router's PIN field displays the fixed PIN that you use to configure the router's WiFi settings from another platform through WPS.
6. To disable the PIN, clear the **Enable Router's PIN** check box.
   By default, the **Enable Router's PIN** check box is selected and the router's PIN is enabled. For enhanced security, you can disable the router's PIN by clearing the **Enable Router's PIN** check box. However, when you disable the router's PIN, WPS is not disabled because you can still use the physical **WPS** button.

   Note: The PIN function might temporarily be disabled automatically if the router detects suspicious attempts to break into the router's WiFi settings by using the router's PIN through WPS. You can configure the number of times a failed PIN connection is allowed before the PIN function is disabled.
7. To allow the WiFi settings to be changed automatically when you use WPS, clear one or both of the **Keep Existing Wireless Settings** check boxes.
   By default, both **Keep Existing Wireless Settings** check boxes are selected. We recommend that you leave these check boxes selected. If you clear a check box, the next time a new WiFi client uses WPS to connect to the router, the router's associated WiFi settings change to an automatically generated random SSID and passphrase.

Clear a **Keep Existing Wireless Settings** check box only if you want to allow the WPS process to change the associated SSID and passphrase for WiFi access.

WARNING: If you clear a **Keep Existing Wireless Settings** check box and use WPS to add a computer or mobile device to the router's WiFi network, the associated SSID and passphrase are automatically generated and other WiFi devices that are already connected to the router's WiFi network might be disconnected.

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

Manage Advanced WiFi Settings

For most WiFi networks, the advanced WiFi settings work fine and you do not need to change the settings.

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

To manage the advanced 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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.
   The Advanced Wireless Settings page displays.
5. Enter the settings as described in the following table.
   The descriptions in the table apply to both the Wireless Network (2.4GHz b/g/n) section and the Wireless Network (5GHz a/n/ac) section.

Field	Description
Fragmentation Length (256-2346)	The fragmentation length (the default is 2346), the CTS/RTS threshold (the default is 2347), and the preamble mode (the default is Long Preamble) are reserved for WiFi testing and advanced configuration only. Do not change these settings unless directed by NETGEAR support or unless you are sure what the consequences are. Incorrect settings might disable the WiFi function of the router unexpectedly.
CTS/RTS Threshold (1-2347)	
Preamble Mode	

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

Specify How the Router Manages WiFi Clients

A WiFi client is any computer or mobile device that connects to the router's WiFi network. The router uses airtime fairness, implicit beamforming, and MU-MIMO to manage its WiFi clients. Airtime fairness and implicit beamforming are enabled by default, but you can disable them. MU-MIMO is disabled by default, but you can enable it.

Manage Airtime Fairness

Airtime fairness ensures that all clients receive equal time on the network. Network resources are divided by time, so if five clients are connected, they each get one-fifth of the network time. The advantage of this feature is that your slowest clients do not control network responsiveness. This feature is enabled by default, but you can disable it.

To disable airtime fairness:

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

The Advanced Wireless Settings page displays.

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

   If you connected over WiFi to the network, you are disconnected from the network and must reconnect.

Manage Implicit Beamforming

Implicit beamforming contrasts with explicit beamforming, which means that 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 signal. 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.
   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 connected over WiFi to the network, you are disconnected from the network and must reconnect.

Manage MU-MIMO

Multiuser multiple input, multiple output (MU-MIMO) improves performance when multiple MU-MIMO-capable WiFi clients transfer data at the same time. WiFi clients must support MU-MIMO, and they must be connected to a 5 GHz WiFi band. This feature is disabled by default, but you can enable it.

To enable 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.
   The Advanced Wireless Settings page displays.
5. Scroll to the bottom of the page and select the **Enable MU-MIMO** check box.
6. Click the **Apply** button.
   Your settings are saved.
   If you connected over WiFi to the network, you are disconnected from the network and must reconnect.

Set Up a WiFi Bridge Between the Router and Another Device

You can use the router as a WiFi bridge and connect multiple devices with WiFi, for example, at the faster 802.11ac speed. To do this, you need another WiFi router or access point (AP) in addition to the router: One device is connected to the Internet over a DSL or cable modem and the other one functions as a WiFi bridge. You can connect the router to the Internet modem and use the router or AP as a WiFi bridge (assuming that the router or AP is capable of functioning as a WiFi bridge), or the other way around—connect the router or AP to the Internet modem, and use the router as a WiFi bridge.

Setting up a WiFi bridge with two routers offers the following benefits:

- You can take advantage of gigabit WiFi speeds on current devices.
- Use gigabit WiFi for applications such as video and gaming.
- Connect multiple devices such as a NAS, Smart TV, NeoTV, Blu-ray player, and game consoles at gigabit WiFi speeds using a WiFi link.
- Avoid the need for separate WiFi adapters for each device.

For example, you could install the first router in a room such as a home office where your Internet connection is located.

Then set up the second router as a WiFi bridge and place it in a different room such as the room where your home entertainment center is located. Cable the router that functions as a WiFi bridge to your Smart TV, DVR, game console, or Blu-ray player, and use its 802.11ac WiFi connection to the first router.

The router that is connected to the Internet modem does not require any special setup because the router that functions as a WiFi bridge connects to an existing SSID as a WiFi client, just like any other WiFi clients.

To set up the router as a WiFi bridge:

1. Make a note of the WiFi settings of the other router that is connected to the Internet modem.

   You must know the SSID, WiFi security mode, WiFi password, and operating frequency (either 2.4 GHz or 5 GHz).

2. Launch a web browser from a computer or mobile device that is connected to the network of the router that you are setting up as a WiFi bridge.
3. Enter **http://www.routerlogin.net**.

   A login window opens.

4. Enter the router user name and password.

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

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.

   The Advanced Wireless Settings page displays.

6. Scroll to the very bottom and select the **Use other operation mode** check box.
7. Select the **Enable Bridge mode** radio button.

   The bridge mode settings displays on the page.

8. Click the **setup bridge mode wireless settings** button.

The Wireless Settings page displays.

9. Enter the WiFi settings of the router that is connected to the Internet modem (that is, the *other* router):
   a. From the **Choose a Wireless Network** menu, select the WiFi band that the other router.
      For 802.11ac mode, both routers must use the same 5 GHz band.
   b. In the **Name (SSID)** field, enter the WiFi network name (SSID) that the other router is using.
   c. In the Security Options section, select the radio button for the WiFi security that the other router is using.
   d. If prompted, type the passphrase (the WiFi password that you must use to connect with WiFi to the other router).

10. Click the **Apply** button.
    Your settings are saved and the pop-up window closes.

11. To change the name of the router, enter a new name in the **Device Name** field.
    By default, the device name is the router model. If you set up the router as a WiFi bridge and you want to distinguish it from the name of the router that is connected to the Internet modem, you could, for example, change the name to *WiFi bridge* or something similar.

12. To let the router that functions as the WiFi bridge get an IP address and DNS addresses dynamically from the router that is connected to the Internet modem, leave the **Get IP Address Dynamically** and **Get DNS Server Address Dynamically** check boxes selected.
    We recommend that you leave the **Get IP Address Dynamically** and **Get DNS Server Address Dynamically** check boxes selected. However, if you are sure that you must use a static IP address, us an IP address from the LAN IP address pool of the router that is connected to the Internet modem. To specify a static IP address for the router that functions as the WiFi bridge, do the following:
    a. Clear the **Get IP Address Dynamically** check box.
       The **Get DNS Server Address Dynamically** check box is automatically cleared.
    b. Enter all static IP address information and, if applicable, static DNS address information.

13. Click the **Apply** button.
    Your settings are saved. The router restarts with a new IP address.

14. To reconnect, close your browser, relaunch it, and log in to the router by entering **http://www.routerlogin.net**.

    When the router functions as a WiFi bridge, you cannot change its WiFi settings, that is, the settings on the Wireless Network page (**BASIC > Wireless**) are masked out. However, if you want to reverse the configuration, you can disable the WiFi bridge option (that is, clear the **use other operation mode** check box) on the Advanced Wireless Settings page (**ADVANCED > Advanced Setup > Advanced Wireless Settings**).

Use the Router as a WiFi Access Point Only

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

Tip: If you want to change the router's function, use a wired connection to avoid being disconnected when the new function takes effect.

To change the router to access point mode only:

1. Use an Ethernet cable to connect the yellow Internet port on the rear panel of the router to a LAN port on the other router.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.

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

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

   The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Wireless Access Point**.

   The Wireless Access Point page displays.
6. Select the **Enable Access Point Mode** check box.

   The page expands.
7. Scroll down and select the radio button for the IP address setting that you want to use:

- **Get dynamically from existing router**. The other router on the network assigns an IP address to the router while the router functions in access point mode. This is the default setting.
- **Use fixed IP Address (not recommended)**. Use this setting if you want to manually assign a specific IP address to the router while it functions in access point mode. Using this option effectively requires network experience.

Note: To avoid interference with other routers or gateways on 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 or gateway and use the 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 web browser and enter **http://www.routerlogin.net**.

13

Use VPN to Access Your Network

You can use OpenVPN software to remotely access your router using virtual private networking (VPN). This chapter explains how to set up 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 aren't home.

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

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 specify the VPN service:

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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.
   The VPN page displays.
5. Select the **Enable VPN Service** check box.
   By default, the VPN uses the UDP service type and uses port 12974. 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, scroll down to the **Service Port** field, and type the port number that you want to use.
8. Click the **Apply** button.
   Your changes are saved. VPN is enabled in the router, but you must install and set up OpenVPN software on your 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 Your Windows-Based Computer

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

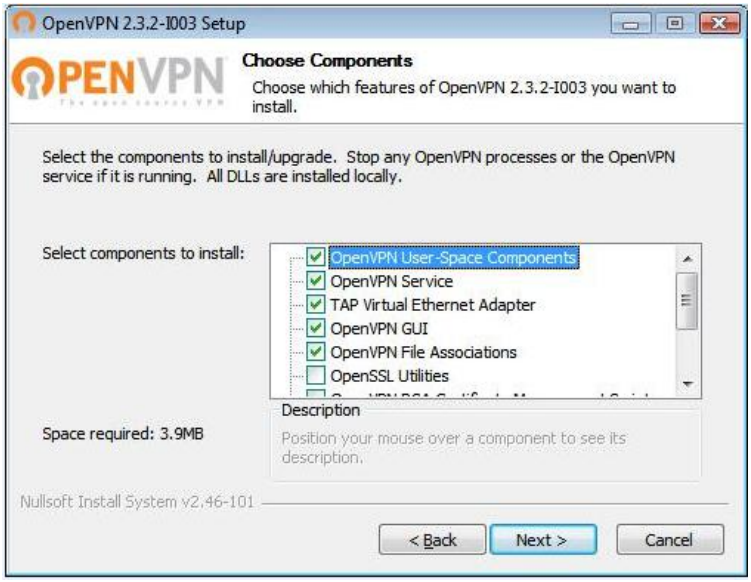
To install VPN client software on your Windows computer:

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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.
   The VPN Service page displays.
5. Make sure that the **Enable VPN Service** check box is selected.
6. Specify any VPN service settings on the page.
   For more information, see Specify VPN Service in the Router on page 167.
7. Click the **For Windows** button to download the OpenVPN configuration files.
8. Visit openvpn.net/index.php/download/community-downloads.html to download the OpenVPN client utility.

9. In the Windows Installer section of the page, double-click the **openVPN-install-xxx.exe** link.
10. Download and install the Open VPN software on your computer, click the **openVPN-install-xxx.exe** file.

    The OpenVPN install window opens.

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



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

    The Windows Security window opens.

15. Click the **Install** button.

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

16. Click the **Finish** button.
17. Unzip the configuration files that you downloaded and copy them to the folder where the VPN client is installed on your device.

    For a client device with Windows 64-bit system, the VPN client is installed at `C:\Program files\OpenVPN\config\` by default.

18. For a client device with Windows, modify the VPN interface name to **NETGEAR-VPN**:
    a. On your computer, go to the Networks page. 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 your Windows-based computer, visit https://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 user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.
   The VPN Service page displays.
5. Make sure that the **Enable VPN Service** check box is selected.
6. Specify any VPN service settings on the page.
   For more information, see Specify VPN Service in the Router on page ?.
7. Click the **For non-Windows** button to download the OpenVPN configuration files.
8. Visit https://tunnelblick.net/index.html to download the OpenVPN client utility for Mac OS X.
9. Download and install the file.

10. 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 ge installed by a user with administrative priviledges.

    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 network.
2. Enter **http://www.routerlogin.net**.

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

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

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.

   The VPN Service page displays.
5. Make sure that the **Enable VPN Service** check box is selected.
6. Specify any VPN service settings on the page.

   For more information, see Specify VPN Service in the Router on page 167.
7. Click the **For Smart Phone** button to download the OpenVPN configuration files.
8. On your iOS device, download and install the OpenVPN Connect app from the Apple app store.
9. 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 network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.
   The VPN Service page displays.
5. Make sure that the **Enable VPN Service** check box is selected.
6. Specify any VPN service settings on the page.
   For more information, see Specify VPN Service in the Router on page 167.
7. Click the **For Smart Phone** button to download the OpenVPN configuration files.
8. On your Android device, download and install the OpenVPN Connect app from the Google Play Store.
9. On your computer, unzip the configuration files that you downloaded and send the files to your Android device.
10. Open the files on your Android device.
11. 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 Your Windows-Based Computer

After you set up the router to use VPN and install the OpenVPN application on your 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.

To open a VPN tunnel:

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 Device and Media

To access a USB device and download files from your Windows-based computer using VPN:

1. On your Windows-based computer, open the Windows file manager and select **Network**.

   Note: See your computer's documentation for information about how to display the network resources.

   The network resources display. The **ReadySHARE** icon displays in the Computer section and the remote router icon displays 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 window.
   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 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 Set Up VPN Client Internet Access in the Router on page 175.
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.

Set Up VPN Client Internet Access in the Router

By default, the router is set up to allow VPN connections only to your home network, but you can change the settings to allow Internet access. Accessing the Internet remotely through a VPN might be slower than accessing the Internet directly.

To allow VPN clients to use your home Internet service:

1. Launch a web browser from a computer or mobile device that is connected to the 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.
   The VPN page displays.
5. Select the **Enable VPN Service** radio button.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **All sites on the Internet & Home Network** radio button.
   When you access the Internet with the VPN connection, instead of using a local Internet service, you use the Internet service from your home network.
7. Click the **Apply** button.
   Your settings are saved.
8. Click the **For Windows** or **For Non Windows** button and download the configuration files for your VPN clients.
9. Unzip the configuration files and copy them to the folder where the VPN client is installed on your device.
   For a client device with Windows 64-bit system, the VPN client is installed at `C:\Program files\OpenVPN\config\` by default.

Block VPN Client Internet Access in the Router

By default, the router is set up to allow VPN connections only to your home network, not to the Internet service for your home network. If you changed this setting to allow Internet access, you can change it back.

To allow VPN clients to access only your home network:

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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.
   The VNP page displays.
5. Select the **Enable VPN Service** radio button.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **Home Network only** radio button.
   This is the default setting. The VPN connection is only to your home network, not to the Internet service for your home network.
7. Click the **Apply** button.
   Your settings are saved.
8. Click **For Windows** or **For Non Windows** button and download the configuration files for your VPN clients.
9. Unzip the configuration files and copy them to the folder where the VPN client is installed on your device.
   For a client device with Windows 64-bit system, the VPN client is installed at `C:\Program files\OpenVPN\config\` by default.

Use VPN to access your Internet service at home

When you're away from home and you access the Internet, you usually use a local Internet service provider. For example, at a coffee shop you might be given a code that lets you use the coffee shop's Internet service account to surf the web.

Nighthawk lets you use a VPN connection to access your own Internet service when you're away from home. You might want to do this if you travel to a geographic location that doesn't support all the Internet services that you use at home. For example, your Netflix account might work at home but not in a different country.

14

Manage Port Forwarding and Port Triggering

You can use port forwarding and port triggering to set up rules for Internet traffic for services and applications. 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 a server is part of your network, you can allow certain types of incoming traffic to reach the server. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

The router can forward incoming traffic with specific protocols to computers on your local network. You can specify the servers for applications and you can also specify a default DMZ server to which the router forwards all other incoming protocols (see Set up a default DMZ server on page 117).

Forward Incoming Traffic for a Default Service or Application

You can forward traffic for a default service or application to a computer on your network.

To forward incoming traffic for a default service or application:

1. Decide which type of service, application, or game you want to provide.
2. Find the local IP address of the computer on your network that will provide the service.

   The server computer must always receive the same IP address. To specify this setting, use the reserved IP address feature. See Manage reserved LAN IP addresses on page 124.
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 user name and password.

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

   The BASIC Home page displays.
6. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.
7. Make sure that the **Port Forwarding** radio button is selected.
8. From the **Service Name** menu, select the service or application.

If the service or application that you want to add is not in the list, create a port forwarding rule with a custom service or application (see Add a Port Forwarding Rule With a Custom Service or Application on page 179).

9. In the **Internal IP Address** field, enter the IP address of the computer that must provide the service or that runs the application.
10. Click the **Add** button.

    Your settings are saved and the rule is added to the table.

Add a Port Forwarding Rule With a Custom Service or Application

The router lists default services and applications that you can use in port forwarding rules. If the service or application is not predefined, you can add a port forwarding rule with a custom service or application.

To add a port forwarding rule with a custom service or application:

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

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

2. 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 BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

   The Port Forwarding / Port Triggering page displays.

6. Make sure that the **Port Forwarding** radio button is selected.
7. Click the **Add Custom Service** button.

   The Ports - Custom Services page displays.

8. Specify a new port forwarding rule with a custom service or application as described in the following table.

Field	Description
Service Name	Enter the name of the custom service or application.
Service Type	Select the protocol (**TCP** or **UDP**) that is associated with the service or application. If you are unsure, select **TCP/UDP**.
External port range	If the service or application uses a single port, enter the port number in the **External port range** field. If the service or application uses a range or ranges of ports, specify the range in the **External port range** field. Specify one range by using a dash between the port numbers. Specify multiple ranges by separating the ranges with commas.
Internal port range	Specify the internal port or ports by one of these methods: • If the external and internal port or ports are identical, leave the **Use the same port range for Internal port** check box selected. • If the service or application uses a single port, enter the port number in the **Internal port range** field. • If the service or application uses a range or ranges of ports, specify the range in the **Internal port range** field. Specify one range by using a dash between the port numbers. Specify multiple ranges by separating the ranges with commas.
Internal IP address	Either enter an IP address in the **Internal IP address** field or select the radio button for an attached device that is listed in the table.

9. Click the **Apply** button.
   Your settings are saved. The rule is added to the table on the Port Forwarding / Port Triggering page.

Change a Port Forwarding Rule

You can change an existing port forwarding rule.

To change a port forwarding rule:

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

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Make sure that the **Port Forwarding** radio button is selected.
6. In the table, select the radio button for the service or application name.
7. Click the **Edit Service** button.
   The Ports - Custom Services page displays.
8. Change the settings.
   For information about the settings, see Add a Port Forwarding Rule With a Custom Service or Application on page 179.
9. Click the **Apply** button.
   Your settings are saved. The changed rule displays in the table on the Port Forwarding / Port Triggering page.

Remove a Port Forwarding Rule

You can remove a port forwarding rule that you no longer need.

To remove a port forwarding rule:

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

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Make sure that the **Port Forwarding** radio button is selected.
6. In the table, select the radio button for the service or application name.
7. Click the **Delete Service** button.
   The rule is removed from the table.

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 / Port Triggering 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, 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 enter the name in the web browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

How the Router Implements the Port Forwarding Rule

The following sequence shows the effects of a port forwarding rule:

1. When you enter the URL www.example.com in your browser, the browser sends a web page request message with the following destination information:

   - **Destination address**. The IP address of www.example.com, which is the address of your router.
   - **Destination port number**. 80, which is the standard port number for a web server process.

2. The router receives the message and finds your port forwarding rule for incoming port 80 traffic.
3. The router changes the destination IP address in the message to 192.168.1.123 and sends the message to that computer.
4. Your web server at IP address 192.168.1.123 receives the request and sends a reply message to your router.

5. 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 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 in your rule and forwards that incoming traffic to that destination.

Port forwarding creates a static mapping of a port number or range of ports to a single local computer. Port triggering can dynamically open ports to any computer when needed and close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance, enable Universal Plug-N-Play (UPnP). See Improve network connections with Universal Plug and Play on page 52.

Add a Port Triggering Rule

The router does not provide default services and applications for port triggering rules. You must define a custom service or application for each port triggering rule.

To add a port triggering rule:

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

The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
   The port triggering settings display.
6. Click the **Add Service** button.
   The Port Triggering Rule page displays.
7. Specify a new port triggering rule with a custom service or application as described in the following table.

Field	Description
Service	
Service Name	Enter the name of the custom service or application.
Service User	From the **Service User** menu, select **Any**, or select **Single address** and enter the IP address of one computer: • **Any**. This is the default setting and allows any computer on the Internet to use this service. • **Single address**. Restricts the service to a particular computer. Enter the IP address in the field that becomes available with this selection from the menu.
Service Type	Select the protocol (**TCP** or **UDP**) that is associated with the service or application.
Triggering Port	Enter the number of the outbound traffic port that must open the inbound ports.
Required Inbound Connection	
Service Type	Select the protocol (**TCP** or **UDP**) that is associated with the inbound connection. If you are unsure, select **TCP/UDP**.
Starting Port	Enter the start port number for the inbound connection.
Ending Port	Enter the end port number for the inbound connection.

8. Click the **Apply** button.
   Your settings are saved and the rule is added to the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

Change a Port Triggering Rule

You can change an existing port triggering rule.

To change a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
   The port triggering settings display.
6. In the Port Triggering Portmap Table, select the radio button for the service or application name.
7. Click the **Edit Service** button.
   The Port Triggering Rule page displays.
8. Change the settings.
   For information about the settings, see Add a Port Triggering Rule on page 183.
9. Click the **Apply** button.
   Your settings are saved. The changed rule displays in the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

Remove a Port Triggering Rule

You can remove a port triggering rule that you no longer need.

To remove a port triggering rule:

1. Launch a web browser from a computer or mobile 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 BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
   The port triggering settings display.
6. In the Port Triggering Portmap Table, select the radio button for the service or application name.
7. Click the **Delete Service** button.
   The rule is removed from the Port Triggering Portmap Table.

Specify the Time-Out for Port Triggering

The time-out period for port triggering controls how long the inbound ports stay open when the router detects no activity. A time-out period is required because the router cannot detect when the service or application terminates.

To specify the time-out for port triggering:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
   The port triggering settings display.
6. In the **Port Triggering Time-out** field, enter a value up to 9999 minutes.
   The default setting is 20 minutes.

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

Disable Port Triggering

By default, port triggering is enabled. You can disable port triggering temporarily without removing any port triggering rules.

To disable port triggering:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
   A login window opens.
3. Enter the router user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
   The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
   The port triggering settings display.
6. Select the **Disable Port Triggering** check box.
   If this check box is selected, the router does not apply port triggering rules even if you specified them.
7. Click the **Apply** button.
   Your settings are saved.

Application Example: Port Triggering for Internet Relay Chat

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 also 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 WiFi settings

Make sure that the WiFi settings on the WiFi-enabled computer or mobile device and the router match exactly. The WiFi network name (SSID) and WiFi security settings of the router and the computer or mobile device must match exactly. WiFi passwords are case sensitive.

If you set up an access control list, you must add the MAC address of each computer and mobile device to the router's access control list.

Check the network settings

If your computer or mobile device cannot connect to the router, make sure that the network settings of the computer or mobile device are correct. Computers and mobile devices must use network IP addresses on the same network as the router. By default, almost all computers and mobile devices are set up to obtain an IP address automatically using DHCP.

Some Internet service providers require you to use the MAC address of the computer initially registered on the account, but this is an unusual situation. You can view the MAC address on the Attached Devices page of the router web interface.

Troubleshoot with the LEDs

By default, the router uses standard LED settings.

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 lit.
    - The Internet LED is lit.
    - The WiFi LED is lit (unless you turned off the WiFi radio).

You can use the LEDs on the front panel of the router for troubleshooting.

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.

Internet or Ethernet LAN port LEDs are off

If the Internet LED or Ethernet LAN port LEDs do not light when an 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.

You cannot log in to the router

If you are unable to log in to the router from a computer or mobile device on your local network, check the following:

- If you are using an Ethernet-connected computer, check the cable connection between the computer and the router.
- If you are using a WiFi-enabled computer or mobile device, check the WiFi connection between the computer or mobile device and the router.
- Make sure that you are using the correct login information. The user name is **admin**. The password is the one that you specified the first time that you logged in. (The default password is **password**.) The user name and password are case-sensitive. Make sure that Caps Lock is off when you enter this information.
- Try quitting the browser and launching it again.
- 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.
- Make sure that the IP address of your computer or mobile device is in the same subnet as the router. If you are using the recommended addressing scheme, the IP address of your computer or mobile device is in the range of 192.168.1.2 to 192.168.1.254.
- If the IP address of your computer or mobile device is shown as 169.254.x.x, the computer or mobile device could not reach the router's DHCP server and the Windows or Mac operating system generated and assigned an IP address. Such an autogenerated IP address is in the range of 169.254.x.x. If your IP address is in this

range, check the connection from the computer or mobile device to the router, and reboot your computer or mobile device.

- 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.

  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.

- 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 a WAN 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. You can determine whether the request was successful using the router web interface.

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 https://www.netgear.com/.
3. Enter **http://www.routerlogin.net**.
   A login window opens.
4. Enter the router admin user name and password.
   The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
   The BASIC Home page displays.
5. Click the **ADVANCED** tab.
   The ADVANCED Home page displays.
6. Check to see that an IP address is shown for the Internet port. 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 modem to recognize your new router by restarting your network. For more information, see Sequence to restart your network on page 190.

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.
  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, you no longer need to run that software after installing your router.

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 Internet service provider (ISP) sets a usage limit, they might charge you for the overage.

- 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. Restart the computer and verify that the router address (www.routerlogin.net) is listed by your computer as the default gateway address.

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 over WiFi to the router, try to isolate the problem:

- Does the WiFi device or computer that you are using find your WiFi network?
  If not, check the WiFi LED on 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.
  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. (By default, SSID broadcast is enabled.)
- Does your WiFi device support the security that you are using for your WiFi network (WPA, WPA2, or WPA3)?

- 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, and select **BASIC > Wireless**.

Note: Be sure to click the **Apply** button if you change settings.

If your WiFi device finds your network but the signal strength is weak, check these conditions:

- Is your router too far from your computer or too close? Place your computer 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 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 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.

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 196.
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.

A

Supplemental Information

This appendix includes technical information about your router.

The appendix covers the following topics:

Factory Settings

You can reset the router to the factory default settings that are shown in the following table.

For information about resetting the router to its factory settings, see Return the router to its factory default settings on page 141.

The following table shows the factory default settings for your router.

Table 3. Router factory default settings

Feature	Default Settings
Router login	
User login URL	www.routerlogin.net (or www.routerlogin.com or 192.168.1.1)
User name (case-sensitive)	admin
Login password (case-sensitive)	password
Internet connection	
WAN MAC address	Use default hardware address
WAN MTU size	Determined by the protocol that is used for the Internet connection (see Manage the MTU size on page 42)
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 zone	North America: Pacific Standard Time Europe: GMT Other continents: Varies by region
Time adjusted for daylight saving time	Disabled

Table 3. Router factory default settings (Continued)

Feature	Default Settings
Firewall and WAN security	
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
Port scan and DoS protection	Enabled
Respond to ping on Internet port	Disabled
IGMP proxying	Disabled
VPN pass-through	Enabled
SIP ALG	Enabled
NAT filtering	Secured
Main WiFi network	
WiFi communication	Enabled
SSID name	See the router label
Security	WPA2-PSK (AES)
WiFi passphrase	See the router label
Country/region	North America: United States Europe: Europe Other continents: Varies by region
RF channel	The available channels depend on the region.
Transmission speed	Auto Note that throughput can vary: Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, affect the data throughput rate.
Link rate	300+1300 AC1600
Transmit power	100%, nonconfigurable
Guest WiFi network	
WiFi communication	Disabled

Table 3. Router factory default settings (Continued)

Feature	Default Settings
SSID name	2.4 GHz band: NETGEAR_Guest 5 GHz band: NETGEAR-5G_Guest
Security	None (open network)
Allow guests to access main network	Disabled
General WiFi settings	
Radio transmission power	100%, nonconfigurable
20/40 MHz coexistence	Enabled
Fragmentation length	2346
CTS/RTS threshold	2347
Preamble mode	Long Preamble
WPS	
WPS capability	Enabled
Router's PIN	Enabled. See the router web interface (select **ADVANCED > Advanced Setup > Advanced Wireless Settings**).
Keep existing wireless settings	Enabled

Technical Specifications

The following table shows the technical specifications for the router.

Table 4. Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, Dynamic DNS, UPnP, and SMB
Power adapter	North America: 120V, 60 Hz, input All regions: 12V @ 1.5A output
Dimensions	9.27 x 5.94 x 2.14 in. (235.51 x 150.76 x 54.5 mm)
Weight	0.75 lb (340 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
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
WiFi	Maximum WiFi signal rate complies with the IEEE 802.11 standard. Note that NETGEAR makes no express or implied representations or warranties about this product's compatibility with any future WiFi standards. 802.11ac 1300 Mbps is approximately 4x faster than 802.11n 300 Mbps. Up to 1300 Mbps WiFi speeds achieved when connecting to other 802.11ac 1300 Mbps devices.
USB	One USB 2.0 port
Radio data rates	Auto-rate sensing
Data encoding standards	IEEE 802.11 b/g/n 2.4 GHz IEEE 802.11 a/n/ac 5.0 GHz
Maximum computers per WiFi network	Limited by the amount of WiFi network traffic generated by each node (typically 50–70 nodes)

Table 4. Router specifications (Continued)

Feature	Description
Operating frequency range	2.4 GHz band • US: 2.412–2.462 GHz • Europe: 2.412–2.472 GHz • Australia: 2.412–2.472 GHz • Japan: 2.412–2.472 GHz 5 GHz band • US: 5.18–5.24 + 5.745–5.825 GHz • Europe: 5.18–5.24 GHz • Australia: 5.18–5.24 + 5.745–5.825 GHz • Japan: 5.18–5.24 GHz
802.11 security	WPA2-PSK, WPA-PSK, WPA/WPA2 (mixed mode), WPA/WPA2 Enterprise, and WEP