

NETGEAR®

User Manual

AC750 WiFi Router

Model R6020

May 2019
202-11750-04

NETGEAR, Inc.

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

Support

Thank you for purchasing this NETGEAR product.

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

Compliance and Conformity

For regulatory compliance information including the EU Declaration of Conformity, visit <https://www.netgear.com/about/regulatory/>. See the regulatory compliance document before connecting the power supply.

Trademarks

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

Contents

Chapter 1 Hardware Overview of the Router

Unpack Your Router.....	9
LED Descriptions.....	10
Ports, Buttons, and Connectors on the Back Panel.....	10
Router Label.....	12
Position the Router.....	12
Cable Your Router.....	13

Chapter 2 Connect to the Network and Access the Router

Connect to the Router.....	16
Connect to the Router Through an Ethernet Cable.....	16
Join the WiFi Network of the Router.....	16
Manual Method.....	16
Wi-Fi Protected Setup Method.....	17
Types of Logins.....	18
Use a Web Browser to Access the Router.....	18
Automatic Internet Setup.....	18
Log In to the Router.....	20
Change the Language.....	20

Chapter 3 Specify Your Internet Settings

Use the Internet Setup Wizard.....	22
Manually Set Up the Internet Connection.....	22
Specify an Internet Connection Without a Login.....	22
Specify an Internet Connection That Uses a Login and PPPoE Service.....	24
Specify an Internet Connection That Uses a Login and PPTP Service.....	26
Specify an Internet Connection That Uses a Login and L2TP Service.....	27
Specify an IPv6 Internet Connection.....	29
IPv6 Internet Connections and IPv6 Addresses.....	29
Use Auto Detect for an IPv6 Internet Connection.....	30
Use Auto Config for an IPv6 Internet Connection.....	31
Set Up an IPv6 6to4 Tunnel Internet Connection.....	33
Set Up an IPv6 Pass-Through Internet Connection.....	34

Set Up a Fixed IPv6 Internet Connection.....	35
Set Up an IPv6 DHCP Internet Connection.....	36
Set Up an IPv6 PPPoE Internet Connection.....	37
Manage the MTU Size.....	39
MTU Concepts.....	39
Change the MTU Size.....	40
Chapter 4 Control Access to the Internet	
Enable access control to allow or block access to the Internet....	43
Manage network access control lists.....	44
Use Keywords to Block Internet Sites.....	45
Set Up Blocking.....	45
Remove a Keyword or Domain From the Blocked List.....	46
Remove All Keywords and Domains From the Blocked List....	47
Specify a Trusted Computer.....	47
Set Up a Schedule for Keyword Blocking and Outbound Firewall Rules.....	48
Chapter 5 Manage the Basic WiFi Network Settings	
Manage the Basic WiFi Settings and WiFi Security of the Main Network.....	51
View or Change the Basic WiFi Settings and WiFi Security Settings.....	51
Configure WEP Legacy WiFi Security.....	57
Configure WPA/WPA2 Enterprise WiFi Security.....	59
Use WPS to Add a Device to the WiFi Network.....	61
Use WPS With the Push Button Method.....	61
Use WPS With the PIN Method.....	62
Manage the Basic WiFi Settings and WiFi Security of the Guest Network.....	63
Enable or Disable the WiFi Radios.....	67
Chapter 6 Manage the WAN and LAN Network Settings	
View or Change WAN Settings.....	69
Set Up a Default DMZ Server.....	70
Manage IGMP Proxying.....	71
Manage VPN Pass-Through.....	71
Manage NAT Filtering.....	72
Manage the SIP Application-Level Gateway.....	73
Manage the LAN IP Address Settings.....	74
Manage the Router Information Protocol Settings.....	75
Manage the DHCP Server Address Pool.....	76
Manage Reserved LAN IP Addresses.....	77
Reserve a LAN IP Address.....	77

Change a Reserved IP Address.....	78
Remove a Reserved IP Address Entry.....	78
Disable the Built-In DHCP Server.....	79
Change the Router's Device Name.....	80
Set Up and Manage Custom Static Routes.....	81
Set Up a Static Route.....	81
Change a Static Route.....	83
Remove a Static Route.....	83
Set Up a Bridge for a Port Group or VLAN Tag Group.....	84
Set Up a Bridge for a Port Group.....	84
Set Up a Bridge for a VLAN Tag Group.....	85
Improve Network Connections With Universal Plug-N-Play.....	87

Chapter 7 Manage the Router

Update the Firmware of the Router.....	90
Check for New Firmware and Update the Router.....	90
Manually Upload New Firmware and Update the Router.....	91
Change the admin Password.....	92
Set Up Password Recovery.....	93
Recover the admin Password.....	94
Manage the Configuration File of the Router.....	94
Back Up the Settings.....	94
Restore the Settings.....	95
Return the Router to Its Factory Default Settings.....	96
Use the Reset Button.....	96
Erase the Settings.....	97
View the Status and Statistics of the Router.....	98
View Information About the Router and the Internet and WiFi Settings.....	98
Display Internet Port Statistics.....	99
Check the Internet Connection Status.....	100
Manage the Activity Log.....	101
View, Email, or Clear the Logs.....	101
Specify Which Activities Are Logged.....	102
View Devices Currently on the Network.....	102

Chapter 8 Manage the Advanced WiFi Features

Set Up a WiFi Schedule.....	105
Manage the WPS Settings.....	106
Manage Advanced WiFi Settings.....	107
Use the Router as a WiFi Access Point Only.....	108

Chapter 9 Manage Port Forwarding and Port Triggering

Manage Port Forwarding to a Local Server for Services and Applications.....	111
Forward Incoming Traffic for a Default Service or Application.....	111
Add a Port Forwarding Rule With a Custom Service or Application.....	112
Change a Port Forwarding Rule.....	113
Remove a Port Forwarding Rule.....	114
Application Example: Make a Local Web Server Public.....	115
How the Router Implements the Port Forwarding Rule.....	115
Manage Port Triggering for Services and Applications.....	116
Add a Port Triggering Rule.....	116
Change a Port Triggering Rule.....	118
Remove a Port Triggering Rule.....	118
Specify the Time-Out for Port Triggering.....	119
Disable Port Triggering.....	120
Application Example: Port Triggering for Internet Relay Chat.....	120

Chapter 10 Troubleshooting

Reboot the Router From Its Web Interface.....	123
Quick Tips.....	123
Sequence to Restart Your Network.....	123
Check Ethernet Cable Connections.....	124
WiFi Settings.....	124
Network Settings.....	124
Troubleshoot With the LEDs.....	124
Standard LED Behavior When the Router Is Powered On.....	124
Power LED Is Off or Blinking.....	125
Power LED Stays Amber.....	125
Internet or Ethernet LEDs Are Off.....	125
WiFi LED Is Off.....	126
You Cannot Log In to the Router.....	126
You Cannot Access the Internet.....	127
Check the WAN IP Address.....	127
Troubleshoot PPPoE.....	128
Troubleshoot Internet Browsing.....	129
Changes Are Not Saved.....	130
Troubleshoot WiFi Connectivity.....	130
Troubleshoot Your Network Using the Ping Utility.....	131
Test the LAN Path to Your Router.....	131
Test the Path From Your Computer to a Remote Device.....	132

Appendix A Supplemental Information

Factory Settings.....	134
Technical Specifications.....	137

1

Hardware Overview of the Router

This chapter contains the following sections:

- [Unpack Your Router](#)
- [LED Descriptions](#)
- [Ports, Buttons, and Connectors on the Back Panel](#)
- [Router Label](#)
- [Position the Router](#)
- [Cable Your Router](#)

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.

In this manual, the terms *wireless* and *WiFi* are interchangeable.

Unpack Your Router

The box contains the following items.



Figure 1. Package contents

Table 1. Legend





1.	Router
2.	Ethernet cable
3.	Power adapter

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

LED Descriptions

The following table describes the LEDs on the router.

Table 2. LED descriptions

LED	Description
Power LED 	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.
WiFi LED 	Solid green. The wireless radio is operating. Off. The wireless radio is off.
Internet LED 	Solid green. The Internet connection is ready. Off. No Ethernet cable is connected between the router and the modem.
Ethernet ports 1-4 LED 	Solid green. A powered-on device is connected to the Ethernet port. Off. No device is connected to this Ethernet port.

Ports, Buttons, and Connectors on the Back Panel

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



Figure 2. Router back panel

In addition to the two antennas, the back panel contains the following components:

- **Reset/WPS button.** This button can be used to reboot and reset the router and connect WPS-enabled devices to the router depending on how long the button is pressed:
 - **Reboot the router.** Press the button for less than 5 seconds to reboot the router.
 - **Connect WPS-enabled devices.** Press the button for about 5 to 10 seconds until the WiFi LED blinks amber.
 - **Reset the router to its factory default settings.** Press the button for more than 10 seconds until all the LEDs blink green.
- **Ethernet LAN ports.** Use the four Fast Ethernet RJ-45 LAN ports to connect the router to LAN devices.
- **Internet WAN port.** Use the blue Fast Ethernet RJ-45 WAN port to connect the router to a modem.
- **Power On/Off button.** Press the **Power On/Off** button to provide power to the router.

Note: Depending on your region, your router might not have a **Power On/Off** button.

- **DC power connector.** Connect the power adapter that came in the product package to the DC power connector.

Router Label

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

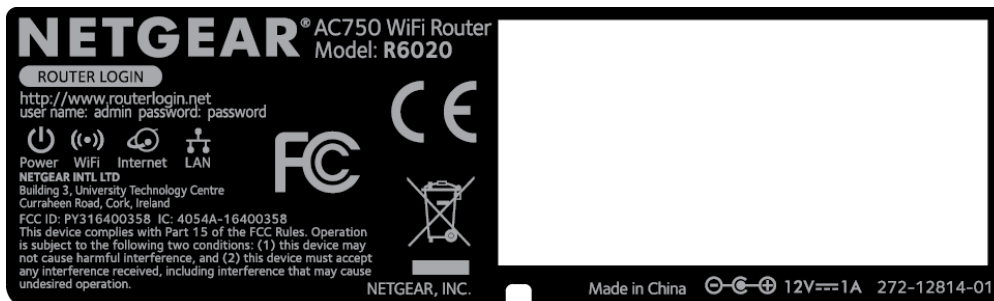


Figure 3. Router label

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:

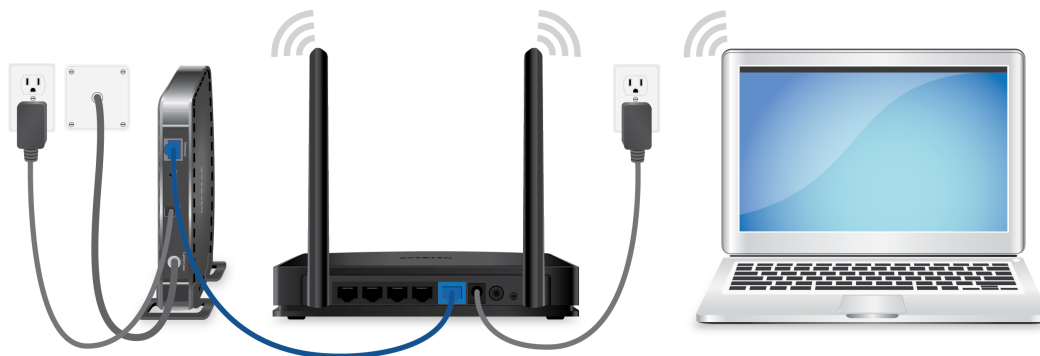


Figure 4. Router cabling

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 blue Ethernet cable that came with your router.
4. Connect the power adapter to your router and plug the power adapter into an outlet.
5. If the Power LED does not light, press the **Power On/Off** button on the back panel of the 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 describes the ways you can connect and how to access the router and log in.

The chapter contains the following sections:

- [Connect to the Router](#)
- [Use a Web Browser to Access the Router](#)
- [Change the Language](#)

Connect to the Router

During and after installation, 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 of your computer so that it uses Dynamic Host Configuration Protocol (DHCP).

Connect to the Router Through an Ethernet Cable

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

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

1. Make sure that the router is receiving power (its Power LED is lit).
2. Connect an Ethernet cable to an Ethernet port on your computer.
3. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports.
Your computer connects to the local area network (LAN). A message might display on your computer screen to notify you that an Ethernet cable is connected.

Join the WiFi Network of the Router

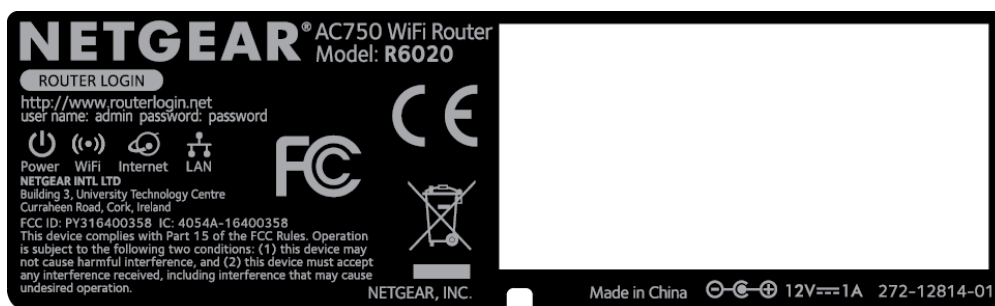
Choose either the manual or the WPS method to add a WiFi device such as a WiFi-enabled computer, an iPhone, an iPad, another mobile device, or a gaming device to the WiFi network of the router.

Manual Method On the WiFi device that you want to connect to the router, you can use the software application that manages your WiFi connections.

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

1. Make sure that the router is receiving power (its Power LED is lit).
2. On the WiFi device that you want to connect to your router, open the software application that manages your WiFi connections.
This software scans for all WiFi networks in your area.
3. Look for the router's network and select it.

If you did not change the name of the network during the setup process, look for the default WiFi network name (SSID) and select it. The default SSID is on the router label.



4. Enter the router WiFi password.
The default WiFi password (also referred to as the *network key* or *passphrase*) is also on the router label.
5. Click the **Connect** button.
The device connects to the WiFi network of the router.

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

To use WPS to connect a computer or mobile device to the WiFi network of the router:

1. Make sure that the router is receiving power (its Power LED is lit).
2. Check the WPS instructions for your computer or mobile device.
3. Press the **Reset/WPS** button of the router for about 5 to 10 seconds until the WiFi LED blinks amber.
4. Within two minutes, press the **WPS** button on your computer or mobile device, or follow the WPS instructions that came with the device.

The WPS process automatically sets up the device with the network password and connects the device to the WiFi network of the router.

For more information, see [Use WPS to Add a Device to the WiFi Network](#) on page 61.

Types of Logins

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

Several types of logins are associated with the router:

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

Use a Web Browser to Access the Router

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

Automatic Internet Setup

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

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

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

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

Using the installation assistant, basic setup takes about 15 minutes to complete.

To automatically set up your router:

1. Turn the router on by pressing the **On/Off** button.
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 browser goes to **http://www.routerlogin.net** and the NETGEAR installation assistant displays.
4. If the browser does not display the NETGEAR installation assistant, enter **http://www.routerlogin.net** in the address field.
5. Follow the onscreen instructions.
The router connects to the Internet.
6. If the browser does not display the installation assistant page, do the following:
 - Make sure that the computer is connected to one of the four 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.
7. 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 127.
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 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 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.

Change the Language

By default, the language is set as Auto. You can change the language.

To change the language:

1. Launch a web browser from a computer or mobile device that is connected to the 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. 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 the NETGEAR installation assistant to detect the Internet connection when you first access the router with a web browser. You can also customize or specify your Internet settings.

This chapter contains the following sections:

- [Use the Internet Setup Wizard](#)
- [Manually Set Up the Internet Connection](#)
- [Specify an IPv6 Internet Connection](#)
- [Manage the MTU Size](#)

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 installation assistant pages that displays 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 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 > 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 22).
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

You can manually specify the connection settings for an Internet service for which you do not need to log in.

Use the information that your 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 an Internet service for which you do not need to log in:

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 **Internet**.
The Internet Setup page displays.
5. Leave the Does your Internet connection require a login? **No** radio button selected.
6. If your Internet connection requires an account name or host name, type it in the **Account Name (If Required)** field.
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.

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 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 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 **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 127.

Specify an Internet Connection That Uses a Login and PPTP Service

You can manually specify the connection settings for a PPTP Internet service for which you must log in. Use the information that your 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 Internet service for which you must log in:

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 **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** 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.
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.

Specify an Internet Connection That Uses a Login and L2TP Service

You can manually specify the connection settings for an L2TP Internet service for which you must log in. Use the information that your 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 an 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 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 **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 **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**, **IP Subnet Mask**, **Server Address**, and **Gateway IP Address** fields.

If your ISP did not give you IP addresses, a connection ID, or name, leave these fields blank.

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.

Specify an IPv6 Internet Connection

The router supports many different types of IPv6 Internet connections for which you can specify the settings manually.

IPv6 Internet Connections and IPv6 Addresses

The router can support an IPv6 Internet connection through the following connection types:

- **Auto Detect.** For information, see [Use Auto Detect for an IPv6 Internet Connection](#) on page 30.
- **Auto Config.** For information, see [Use Auto Config for an IPv6 Internet Connection](#) on page 31.
- **6to4 tunnel.** For information, see [Set Up an IPv6 6to4 Tunnel Internet Connection](#) on page 33.
- **Pass-through.** For information, see [Set Up an IPv6 Pass-Through Internet Connection](#) on page 34.
- **Fixed.** For information, see [Set Up a Fixed IPv6 Internet Connection](#) on page 35.
- **DHCP.** For information, see [Set Up an IPv6 DHCP Internet Connection](#) on page 36.
- **PPPoE.** For information, see [Set Up an IPv6 PPPoE Internet Connection](#) on page 37.

Which connection type you must use depends on your IPv6 ISP. Follow the directions that your IPv6 ISP gave you.

- If your ISP did not provide details, use the 6to4 tunnel connection type (see [Set Up an IPv6 6to4 Tunnel Internet Connection](#) on page 33).
- If you are not sure what type of IPv6 connection the router uses, use the Auto Detect connection type, which lets the router detect the IPv6 type that is in use (see [Use Auto Detect for an IPv6 Internet Connection](#) on page 30).

- If your Internet connection does not use pass-through, a fixed IP address, DHCP, or PPPoE but is IPv6, use the Auto Config connection type, which lets the router autoconfigure its IPv6 connection (see [Use Auto Config for an IPv6 Internet Connection](#) on page 31).

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

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

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

Use Auto Detect for an IPv6 Internet Connection

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 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 > IPv6**.
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Detect**.
The IPv6 page displays.
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 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).

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

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

8. Click the **Apply** button.

Your settings are saved.

Use Auto Config for an IPv6 Internet Connection

To set up an IPv6 Internet connection through autoconfiguration:

1. Launch a web browser from a computer or mobile device that is connected to the 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 > IPv6**.
The IPv6 page displays.

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

The IPv6 page displays.

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 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).

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

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

11. Click the **Apply** button.

Your settings are saved.

Set Up an IPv6 6to4 Tunnel Internet Connection

The remote relay router is the device 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 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 > IPv6**.

The IPv6 page displays.

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

The IPv6 page displays.

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 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 an IPv6 pass-through Internet connection:

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 > 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 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 > IPv6**.
The IPv6 page displays.
 5. From the **Internet Connection Type** menu, select **Fixed**.
The IPv6 page displays.
 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 22.)
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 DHCPv6 client function.

- **Auto Config.** This is the default setting.

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

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

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

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

Set Up an IPv6 DHCP Internet Connection

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

1. Launch a web browser from a computer or mobile device that is connected to the 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 > IPv6**.
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **DHCP**.
The IPv6 page displays.

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 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).
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 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 > IPv6**.

The IPv6 page displays.

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

The IPv6 page displays.

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 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).

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 ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
 - A secure website that does not open or displays only part of a web page
 - Yahoo email

- 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.

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

Table 3. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for ping. (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 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 > 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

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:

- [Enable access control to allow or block access to the Internet](#)
- [Manage network access control lists](#)
- [Use Keywords to Block Internet Sites](#)
- [Set Up a Schedule for Keyword Blocking and Outbound Firewall Rules](#)

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.

Manage network access control lists

You can manage network access control lists (ACLs) that block or allow access to the Internet through your router.

To manage devices that are allowed or 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 admin user name and password.
The user name is **admin**. 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** radio button.
6. Click the **View list of allowed devices not currently connected to the network** link.
The list displays.
7. Select the check box for a device.
8. Use the **Add** button, **Edit** button, and **Remove from the list** button as needed.
9. 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 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 > 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 48.
 - **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, repeat [Step 6](#) and [Step 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 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 > 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 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 > 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 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 > 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.

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 45). 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 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 > 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 synchronizes 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.

5

Manage the Basic WiFi Network Settings

This chapter describes how you can manage the basic WiFi network settings of the router. For information about the advanced WiFi settings, see [Manage the Advanced WiFi Features](#) on page 104.

The chapter includes the following sections:

- [Manage the Basic WiFi Settings and WiFi Security of the Main Network](#)
- [Use WPS to Add a Device to the WiFi Network](#)
- [Manage the Basic WiFi Settings and WiFi Security of the Guest Network](#)
- [Enable or Disable the WiFi Radios](#)

For information about setting up an access control list (ACL) and managing WiFi access for enhanced security, see [Control Access to the Internet](#) on page 42.

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 (see [Router Label](#) on page 12).

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 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 **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	<p>From the menu, select the region in which the router operates.</p> <p>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.</p>
Wireless Network (2.4GHz b/g/n)	
Name (SSID)	<p>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.</p> <p>Note: If you change the SSID, enter a 32-character (maximum), case-sensitive name in this field.</p>
Channel	<p>From the Channel menu, select Auto for automatic channel selection or select an individual channel. The default selection is Auto.</p> <p>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.</p> <p>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).</p>

(Continued)

Field	Description
Mode	<p>From the Mode menu, select one of the following modes:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Enable SSID Broadcast	<p>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.</p>
Enable 20/40 MHz Coexistence	<p>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.</p>

(Continued)

Field	Description
Security Options	
This information applies to the 2.4 GHz WiFi network.	
<p>If you change the WiFi security, select one of the following WiFi security options for the router's WiFi network:</p> <ul style="list-style-type: none"> • 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. For information about configuring WEP, see Configure WEP Legacy WiFi Security on page 57. • 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. For information about configuring WPA/WPA2 Enterprise, see Configure WPA/WPA2 Enterprise WiFi Security on page 59. 	
Wireless Network (5GHz a/n/ac)	
Name (SSID)	<p>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.</p> <p>Note: If you change the SSID, enter a 32-character (maximum), case-sensitive name in this field.</p>

(Continued)

Field	Description
Channel	<p>From the Channel menu, select an individual channel for a 5 GHz SSID. The default channel depends on your selection from the Region menu.</p> <p>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.</p> <p>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.</p>
Mode	<p>From the appropriate Mode menu, select one of the following modes for a 5 GHz SSID:</p> <ul style="list-style-type: none"> • Up to 87 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 87 Mbps. • Up to 200 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 200 Mbps. • Up to 433 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 433 Mbps. This mode is the default mode.
Enable SSID Broadcast	<p>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.</p>

(Continued)

Field	Description
Security Options	
This information applies to the 5 GHz WiFi network.	
<p>If you change the WiFi security, select one of the following WiFi security options for the router's WiFi network:</p> <ul style="list-style-type: none"> • 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 <i>not</i> 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. For information about configuring WPA/WPA2 Enterprise, see Configure WPA/WPA2 Enterprise WiFi Security on page 59. 	

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 102.) 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 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 **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 situation disregard [Step 5](#) and go to [Step 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.

Security Options

☐ None
☒ **WEP**
☐ WPA2-PSK [AES]
☐ WPA-PSK [TKIP] + WPA2-PSK [AES]
☐ WPA/WPA2 Enterprise

Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: 64-bit

Security Encryption (WEP)

Key 1: ☒
 Key 2: ☐
 Key 3: ☐
 Key 4: ☐

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 stronger 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 102.) 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 default password is **password**. 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.

Security Options

☐ None
☐ WEP
☐ WPA2-PSK [AES]
☐ WPA-PSK [TKIP] + WPA2-PSK [AES]
☒ WPA/WPA2 Enterprise

Security Options (WPA/WPA2 Enterprise)

Encryption mode: WPA [TKIP] + WPA2 [AES] ▼

Group Key Update Interval: 3600 (Seconds)

RADIUS Server IP Address: . . .

RADIUS server Port: 1812

RADIUS server Shared Secret:

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

Field	Description
Encryption mode	<p>From the Encryption Mode menu, select the encryption mode:</p> <ul style="list-style-type: none"> • 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.
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 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 102.) 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 **Reset/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 and 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 51).

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 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 > WPS Wizard**.

The page displays a description of the WPS method.

5. Click the **Next** button.

The Add WPS Client page displays.

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

6. Either click the  button onscreen or press the **Reset/WPS** button on 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 green.

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 solid green 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 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 > 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.

The Add WPS Client page displays.

7. In the **Enter Client's 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 green.

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 solid green 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 onscreen.

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 51. 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 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 **Guest Network**.
The Guest Network Settings page displays.
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.

(Continued)

Field	Description
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 51). For information about configuring WEP, see [Configure WEP Legacy WiFi Security](#) on page 57.
- **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.

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 <i>password</i> or <i>key</i> .
------------	--

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.
-------------	---

(Continued)

Field	Description
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.

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 <i>password</i> or <i>key</i> .
------------	---

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 102.) 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 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 > 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 solid green.
6. Click the **Apply** button.
Your settings are saved.

6

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:

- [View or Change WAN Settings](#)
- [Set Up a Default DMZ Server](#)
- [Manage IGMP Proxying](#)
- [Manage VPN Pass-Through](#)
- [Manage NAT Filtering](#)
- [Manage the SIP Application-Level Gateway](#)
- [Manage the LAN IP Address Settings](#)
- [Manage the Router Information Protocol Settings](#)
- [Manage the DHCP Server Address Pool](#)
- [Manage Reserved LAN IP Addresses](#)
- [Disable the Built-In DHCP Server](#)
- [Change the Router's Device Name](#)
- [Set Up and Manage Custom Static Routes](#)
- [Set Up a Bridge for a Port Group or VLAN Tag Group](#)
- [Improve Network Connections With Universal Plug-N-Play](#)

View or Change WAN Settings

You can view or configure wide area network (WAN) settings for the Internet port.

To view or change the WAN settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
The WAN Setup page displays.
View or change the following settings:
 - **Default DMZ Server.** This feature is sometimes helpful when you are playing online games or videoconferencing, but it makes the firewall security less effective.
 - **MTU Size (in bytes).** The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. Change the MTU only if you are sure that it is necessary for your ISP connection.
 - **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.
 - **Disable SIP ALG.** Some voice and video communication applications do not work well with the SIP ALG. Disabling the SIP ALG might help your voice and video applications to create and accept a call through the router.
 - **Disable IGMP Proxying.** IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. If you do not need this feature, you can select this check box to disable it.
 - **VPN Passthrough.** VPN connects two secure networks over the Internet. The router supports VPN passthrough for IPSec, PPTP, and L2TP.
5. 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 or application for which you set up a port forwarding or port triggering rule. Instead of discarding this traffic, you can direct the router to forward the traffic to one computer on your network. This computer is called the default DMZ server.

To set up a default DMZ server:

1. 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 > Setup > WAN Setup**.
The WAN Setup page displays.
5. Select the **Default DMZ Server** check box.
6. Enter the IP address of the server.
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 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 > 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 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 > 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 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 > 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 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 > 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 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 > 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 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 > 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 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 > 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.

Reserve a LAN IP Address

You can assign a reserved IP address to a computer or server that requires permanent IP settings.

To reserve an IP address:

1. Launch a web browser from a computer or mobile device that is connected to the 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 > Setup > LAN Setup**.
The LAN Setup page displays.
5. In the Address Reservation section, click the **Add** button.
The Address Reservation page displays.
6. Either select a device from the Address Reservation Table by selecting the corresponding radio button or specify the reserved IP address information:
 - In the **IP Address** field, enter the IP address to assign to the computer or device. Choose an IP address from the router's LAN subnet, such as 192.168.1.x.
 - In the **MAC Address** field, enter the MAC address of the computer or device.
 - In the **Device Name** field, enter the name of the computer or device.

7. Click the **Add** button.

The reserved address is entered into the table on the LAN Setup page.

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

Change a Reserved IP Address

You can change a reserved IP address entry.

To change a reserved IP address entry:

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 > Setup > LAN Setup**.
The LAN Setup page displays.
5. In the Address Reservation section, select the radio button for the reserved address.
6. Click the **Edit** button.
The Address Reservation page displays.
7. Change the settings.
8. Click the **Apply** button.
Your settings are saved.

Remove a Reserved IP Address Entry

You can remove a reserved IP address entry.

To remove a reserved IP address entry:

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 > Setup > LAN Setup**.

The LAN Setup page displays.

5. In the Address Reservation section, select the radio button for the reserved address.

6. Click the **Delete** button.

The address entry 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 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 > 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 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 > 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.
- A metric value of 1 works fine because the ISDN router is on the LAN.

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 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 > 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 .
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 1 through 15. This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1 .

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 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 > 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 information about the settings, see [Set Up a Static Route](#) on page 81.
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 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 > 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 directions on how to set up a bridge for IPTV and Internet service, follow those directions.

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 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 > 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.

VLAN / Bridge Settings

☒ Enable VLAN Tag

☒ By bridge group

Wired Devices		Wireless	
<input type="checkbox"/> Port1	<input type="checkbox"/> Port2	<input type="checkbox"/> WiFi-2.4G	<input type="checkbox"/> WiFi-5G
<input type="checkbox"/> Port3	<input type="checkbox"/> Port4		

☐ By VLAN tag group

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 an 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 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 > 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.

VLAN / Bridge Settings

☒ Enable VLAN Tag

☐ By bridge group

☒ By VLAN tag group

Enable	Name	VLAN ID	Priority	Wired Devices	Wireless
<input checked="" type="checkbox"/>	Internet	10	0	<input checked="" type="checkbox"/> Port1 <input checked="" type="checkbox"/> Port2 <input checked="" type="checkbox"/> Port3 <input checked="" type="checkbox"/> Port4	<input checked="" type="checkbox"/> WiFi-2.4G <input checked="" type="checkbox"/> WiFi-5G

The router includes a default VLAN tag group with the name Internet.

7. Click the **Add** button.
The page adjusts.
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.
<p>Select the check box for a wired LAN port or WiFi port.</p> <p>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.</p> <p>You must select at least one LAN port or WiFi port. You can select more than one port.</p>	

- Click the **Add** button.
The VLAN tag group is added.

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

Improve Network Connections With Universal Plug-N-Play

Universal Plug-N-Play (UPnP) helps devices such as Internet appliances and computers access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance, keep UPnP enabled, which it is by default.

To manage Universal Plug-N-Play:

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

The UPnP page displays.

5. Select the **Turn UPnP On** check box.

By default, this check box is selected. You can disable or enable UPnP for automatic device configuration. 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. Enter 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 detect current device status at the expense of more network traffic. Longer durations can compromise the freshness of the device status but can significantly reduce network traffic.

7. Enter the advertisement time to live in hops.

The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. Hops are the steps a packet takes between routers. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.

8. Click the **Apply** button.

The UPnP Portmap Table displays the IP address of each UPnP device that is accessing the router and which ports (internal and external) that device opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

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

7

Manage the Router

This chapter describes how you can manage the settings for administering and maintaining your router.

The chapter includes the following sections:

- [Update the Firmware of the Router](#)
- [Change the admin Password](#)
- [Set Up Password Recovery](#)
- [Recover the admin Password](#)
- [Manage the Configuration File of the Router](#)
- [Return the Router to Its Factory Default Settings](#)
- [View the Status and Statistics of the Router](#)
- [Manage the Activity Log](#)
- [View Devices Currently on the Network](#)

Update the Firmware of the Router

The router firmware is stored in flash memory.

You can check to see if new firmware is available and update the router to the new firmware. You can also visit the NETGEAR support website, download the firmware manually, and update the router to the new firmware.

Check for New Firmware and Update the Router

For you to check for new firmware, the router must be connected to the Internet.

To check for new firmware and update your router:

1. Launch a web browser from a computer or mobile device that is connected to the 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 > Administration > Firmware Update**
The Firmware Update page displays.
5. Click the **Check** button.
The router detects new firmware if any is available and displays a message asking if you want to download and install it.
6. To download and install the new firmware, click the **Yes** button.
The router locates the firmware, downloads it, 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. Wait until the router finishes restarting and the Power LED turns solid green.

A progress bar might show the progress of the firmware upload process. The firmware upload process takes several minutes. When the upload is complete, your router restarts.

7. Verify that the router is running the new firmware version:
 - a. Launch a web browser from a computer or mobile device that is connected to the network.
 - b. Enter **http://www.routerlogin.net**.
A login window opens.
 - c. 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. The firmware version is stated in the top right, under the **Logout** button.
8. Read the new firmware release notes to determine whether you must reconfigure the router after updating.

Manually Upload New Firmware and Update the Router

Downloading firmware and updating the router are two separate tasks that are combined in the following procedure.

To download new firmware manually and update your router:

1. Visit downloadcenter.netgear.com, locate the support page for your product, and download the new firmware.
2. Read the new firmware release notes to determine whether you must reconfigure the router after updating.
3. Launch a web browser from a computer or mobile device that is connected to the 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 default password is **password**. The user name and password are case-sensitive.
The BASIC Home page displays.
6. Select **ADVANCED > Administration > Firmware Update**.
The Firmware Update page displays.
7. Locate and select the firmware file on your computer:
 - a. Click the **Browse** (or **Choose File**) button.
 - b. Navigate to the firmware file.

The file ends in .chk.

c. Select the firmware file.

8. Click the **Upload** button.

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

A progress bar might show the progress of the firmware upload process. The firmware upload process takes several minutes. When the upload is complete, your router restarts.

9. Verify that the router runs the new firmware version:

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

b. Enter **http://www.routerlogin.net**.
A login window opens.

c. 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. The version firmware is stated in the top right, under the **Logout** button.

Change the admin Password

You can change the default password that is used to log in to the router with the user name admin. This password is not the one that you use for WiFi access.

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.

To set the password for the user name admin:

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 > Administration > Set Password**.
The Set Password page displays.
5. Type the old password, and type the new password twice.
6. To be able to recover the password, select the **Enable Password Recovery** check box.
We recommend that you enable password recovery.
7. If you enable password recovery, select two security questions and provide answers to them.
8. Click the **Apply** button.
Your settings are saved.

Set Up Password Recovery

We recommend that you enable password recovery if you change the password for the router user name admin. Then you can recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers but not in the Safari browser.

To set up password recovery:

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 > 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

To recover your password:

1. In the address field of your browser, enter **<http://www.routerlogin.net>**.
A login window opens.
2. 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.
3. Enter the serial number of the router.
4. Click the **Continue** button.
A window opens requesting the answers to your security questions.
5. Enter the saved answers to your security questions.
6. Click the **Continue** button.
A window opens and displays your recovered password.
7. Click the **Login again** button.
A login window opens.
8. With your recovered password, log in to the router.

Manage the Configuration File of the Router

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 or restore it.

Back Up the Settings

You can save a copy of the current configuration settings.

To back up the router's configuration settings:

1. Launch a web browser from a computer or mobile device that is connected to the 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 > Administration > Backup Settings**.
The Backup Settings page displays.
5. Click the **Back Up** button.
6. Choose a location to store the file on your computer.
The backup file ends in `.cfg`.
7. Follow the directions of your browser to save the file.

Restore the Settings

If you backed up the configuration file, you can restore the configuration from this file.

To restore configuration settings that you backed up:

1. Launch a web browser from a computer or mobile device that is connected to the 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 > Administration > Backup Settings**.
The Backup Settings page displays.
5. Click the **Browse** button and navigate to and select the saved configuration file.
The backup file from which you can restore the configuration ends in `.cfg`.

6. Click the **Restore** button.

The configuration is uploaded to the router. When the restoration is complete, the router reboots. This process takes about two minutes.

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

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.

If you do not know the current IP address of the router, first try to use an IP scanner application to detect the IP address before you reset the router to factory default settings.

To reset the router to factory default settings, you can use either the **Reset/WPS** button on the router or the Erase function. However, if you cannot find the IP address or lost the password to access the router, you must use the **Reset/WPS** button.

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. For a list of factory default settings, see [Factory Settings](#) on page 134.

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. Locate the **Reset/WPS** button on your router.
2. Using a straightened paper clip, press and hold the **Reset** button for more than 10 seconds until all the LEDs blink green.
3. Release the **Reset** button.

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

WARNING: To avoid the risk of corrupting the firmware, do not interrupt the reset. For example, if you are connected to the router's web page, 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 and the Power LED turns solid green.

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 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 > 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 reboots. This process takes about two minutes.

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




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 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. Click the **ADVANCED** tab.
The ADVANCED Home page displays.
The information uses the following color coding:
 - A green flag  indicates that the Internet connection is fine and no problems exist. For a WiFi network, the network is enabled and secured.
 - A red X  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 exclamation mark  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 Internet Port Statistics

To display Internet port statistics:

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. Click the **ADVANCED** tab.
The ADVANCED Home page displays.
5. In the Internet Port pane, click the **Show Statistics** button.
The following information displays:
 - **System Up Time**. The time elapsed since the router was last restarted.
 - **Port**. The statistics for the WAN (Internet), LAN (Ethernet) ports, and WLAN (WiFi) ports. For each port, the pop-up window displays the following information:
 - **Status**. The link status of the port.
 - **TxPkts**. The number of packets transmitted on the port since reset or manual clear.
 - **RxPkts**. The number of packets received on the port since reset or manual clear.
 - **Collisions**. The number of collisions on the port since reset or manual clear.
 - **Tx B/s**. The number of Bytes per second transmitted on the port since reset or manual clear. For this information, the LAN ports are treated as a single port.
 - **Rx B/s**. The number of Bytes per second received on the port since reset or manual clear. For this information, the LAN ports are treated as a single port.
 - **Up Time**. The time elapsed since the port acquired the link.
 - **Poll Interval**. The interval at which the statistics are updated in this window.
6. To change the polling frequency, enter a time in seconds in the **Poll Interval** field and click the **Set Interval** button.

7. 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 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. Click the **ADVANCED** tab.
The ADVANCED Home page displays.
5. In the Internet Port pane, click the **Connection Status** button.
If the ISP assigned an IP address to the router dynamically (the most common situation), the following information displays:
 - **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.

Note: If the Internet connection is PPPoE, PPTP, or L2TP, other information might display.
6. To release (stop) the Internet connection, click the **Release** button.
7. To renew (restart) the Internet connection, click the **Renew** button.

8. To close the window, 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 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 > Administration > Logs**.
The Logs page displays.
The Logs page shows 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.

Specify Which Activities Are Logged

You can specify which activities are logged.

To manage which activities are logged:

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 > 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 the active wired and WiFi devices in both the network to which the router is connected and the router network. If you do not recognize a WiFi device, it might be an intruder.

To display the wired and WiFi devices:

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 **Attached Devices**.

Attached Devices

Go to [Access Control](#) to allow or block devices.

Access Control: Turned Off [Refresh](#)

General Rule: Allow all new devices to connect

Wired Devices

Status	IP Address	MAC Address	Device Name	Connection Type
2.4GHz Wireless Devices (Wireless intruders also show up here)				
Status	SSID	IP Address	MAC Address	Device Name
Allowed	NETGEAR66	192.168.1.2	60:66:66:66:66:66	BUSINESSLAPTOP
5GHz Wireless Devices (Wireless intruders also show up here)				
Status	SSID	IP Address	MAC Address	Device Name
Allowed	NETGEAR66-5G	192.168.1.3	C0:B0:B0:B0:B0:B0	ANDROID

Wired devices are connected to the router with Ethernet cables. Wireless devices are connected to the router through the WiFi network, in either the 2.4 GHz band or one of the 5 GHz bands.

The following table describes the fields that can be displayed.

Field	Description
Status	The status of the device in the network (Allowed or Blocked).
SSID	The name of the WiFi network to which the device is connected.
IP Address	The IP address that the router assigned to the device when it joined the network. This address can change when a device is disconnected and rejoins the network.
MAC Address	The unique MAC address. The MAC address does not change and is usually shown on the product label.
Device Name	The device name, if detected.
Connection Type	The type of connection for the device.

5. To refresh the information onscreen, click the **Refresh** button.

The information onscreen is updated.

8

Manage the Advanced WiFi Features

This chapter describes how you can manage the advanced WiFi features of the router. For information about the basic WiFi settings, see [Manage the Basic WiFi Network Settings](#) on page 50.

The chapter includes the following sections:

- [Set Up a WiFi Schedule](#)
- [Manage the WPS Settings](#)
- [Manage Advanced WiFi Settings](#)
- [Use the Router as a WiFi Access Point Only](#)

Set Up a WiFi Schedule

You can turn off the WiFi signal from your router at times when you do not need a WiFi connection. For example, you might turn it off for the weekend if you leave town. 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 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 > 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. To activate the schedule, select the **Turn off wireless signal by 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 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 > 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 **Reset/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.

For information about viewing this SSID and passphrase, see [View or Change the Basic WiFi Settings and WiFi Security Settings](#) on page 51.

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 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 > 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.
CTS/RTS Threshold (1-2347)	Do not change these settings unless directed by NETGEAR support or unless you are sure what the consequences are. Incorrect settings might disable the WiFi function of the router unexpectedly.
Preamble Mode	

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

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:

- 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.
- Launch a web browser from a computer or mobile device that is connected to the network.
- Enter **http://www.routerlogin.net**.
A login window opens.
- 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.
- Select **ADVANCED > Advanced Setup > Wireless Access Point**.
The Wireless Access Point page displays.
- 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>**.

9

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](#)
- [Manage Port Triggering for Services and Applications](#)

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 70).

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 77.
3. Launch a web browser from a computer or mobile device that is connected to the 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 default password is **password**. 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 112).

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 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 default password is **password**. 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: <ul style="list-style-type: none"> • 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.

- 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:

- Launch a web browser from a computer or mobile device that is connected to the network.
- Enter **http://www.routerlogin.net**.
A login window opens.
- 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. 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 112.

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 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. 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.

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 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-N-Play](#) on page 87.

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 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. Click the **Add Service** button.
The Port Triggering Rules 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	<p>From the Service User menu, select Any, or select Single address and enter the IP address of one computer:</p> <ul style="list-style-type: none"> • 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 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 **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 116.
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 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 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 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 > 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.

10

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:

- [Reboot the Router From Its Web Interface](#)
- [Quick Tips](#)
- [Troubleshoot With the LEDs](#)
- [You Cannot Log In to the Router](#)
- [You Cannot Access the Internet](#)
- [Changes Are Not Saved](#)
- [Troubleshoot WiFi Connectivity](#)
- [Troubleshoot Your Network Using the Ping Utility](#)

Reboot the Router From Its Web Interface

You or NETGEAR technical support can reboot the router from its web interface, either locally or remotely, for example, when the router seems to be unstable or is not operating normally.

To reboot the router from its web interface:

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. Click the **ADVANCED** tab.
The ADVANCED Home page displays.
5. In the Router Information pane, click the **Reboot** button.
A confirmation pop-up window displays.
6. Click the **OK** button.
The router reboots.

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 Ethernet Cable Connections

If your device does not power on, 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 devices are connected to the router by an Ethernet cable, the corresponding numbered router LAN port LEDs light.

WiFi Settings

Make sure that the WiFi settings in the computer or mobile device and router match exactly. The WiFi network name (SSID) and WiFi security settings of the router and computer or mobile device must match exactly.

If you set up an access control list, you must add the MAC address of each computer or mobile device to the router's access control list (see [Enable access control to allow or block access to the Internet](#) on page 43).

Network Settings

Make sure that the network settings of the computer are correct. Wired computers and computers or mobile devices that are connected over WiFi must use network IP addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP.

Some service providers require you to use the MAC address of the computer initially registered on the account, but this is an uncommon situation. You can view the MAC address on the Attached Devices page (see [View Devices Currently on the Network](#) on page 102).

Troubleshoot With the LEDs

By default, the router is set with 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 radios.
-

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 might be corrupted. This can happen if a firmware upgrade 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.

Power LED Stays Amber

When the router is turned on, the Power LED turns amber for up to two minutes and then turns green. If the LED does not turn green, this indicates a problem with the router.

If the Power LED is still amber three minutes after you turn on power to the router, do the following:

- Reboot the router to see if the router recovers.
- If the router does not recover, press and hold the **Reset/WPS** button to return the router to its factory default settings. For more information, see [Use the Reset Button](#) on page 96.

If the error persists, a hardware problem might be the cause. Contact technical support at netgear.com/support.

Internet or Ethernet LEDs Are Off

If either the Internet LED or Ethernet LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connection is secure at the router and at the modem that is connected to the WAN port.
- Make sure that the Ethernet cable connections are secure at the router and at the devices that are connected to the Ethernet ports.

- Make sure that power is turned on to the connected modem and connected devices.
- Be sure that you are using the correct cables.

When you connect the router's WAN port to a modem, use the cable that was supplied with the modem. This cable can be a standard straight-through Ethernet cable or an Ethernet crossover cable.

WiFi LED Is Off

If the WiFi LED stays off, check to see if someone pressed the **WiFi On/Off** button on the router. This button turns the WiFi radios in the router on and off. The WiFi LED is lit when the WiFi radios are turned on.

You Cannot Log In to the Router

If you are unable to log in to the router from a computer on your local network and use the router web interface, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router.
- Make sure that the IP address of your computer is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address is in the range of 192.168.1.2 to 192.168.1.254.
- Make sure that your computer can reach the router's DHCP server. Recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, use an IP scanner application to detect the IP address. If you still cannot find the IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. For more information, see [Return the Router to Its Factory Default Settings](#) on page 96 and [Factory Settings](#) on page 134.
- Make sure that Java, JavaScript, or ActiveX is enabled in your browser. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The user name is **admin**, and the default password is **password**. Make sure that Caps Lock is off when you enter this information.

- If you are attempting to set up your router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services. For example, the router cannot convert DSL or cable data into Ethernet networking information. NETGEAR does not support such a configuration.

You Cannot Access the Internet

If you can access your router but not the Internet, check to see if the router can obtain an IP address from your Internet service provider (ISP).

Check the WAN IP Address

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 **ADVANCED** Home page.

To check the WAN IP address:

1. Launch a web browser from a computer or mobile device that is connected to the network.
2. Select an external site such as netgear.com.
3. Enter **http://www.routerlogin.net**.
A login window opens.
4. 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.
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 123.

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 is does not load any web pages from the Internet, it might be for one or more of the following reasons:

- Your computer might not recognize any DNS server addresses.
A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer, and verify the DNS address. You can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- The router might not be configured as the TCP/IP gateway on your computer. If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address.
- You might be running login software that is no longer needed.
If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**. Other browsers provide similar options.

Troubleshoot PPPoE

If you are using PPPoE, try troubleshooting your Internet connection.

To troubleshoot a PPPoE connection:

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. Click the **ADVANCED** tab.

The ADVANCED Home page displays.

5. In the Internet Port pane, click the **Connection Status** button.

The Connection Status pop-up window opens.

6. Check the information in the Connection Status pop-up window to see if your PPPoE connection is up and working.

If the router is not connected, click the **Connect** button.

The router continues to attempt to connect indefinitely.

7. If you cannot connect after several minutes, the router might be set up with an incorrect service name, user name, or password, or your ISP might be experiencing a provisioning problem.

Unless you connect manually, the router does not authenticate using PPPoE until data is transmitted to the network.

Troubleshoot Internet Browsing

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet, check the following:

- Your computer might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.
Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, restart your computer. Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.
- The router might not be configured as the default gateway on your computer. Reboot the computer and verify that the router address (www.routerlogin.net) is listed by your computer as the default gateway address.
- You might be running login software that is no longer needed. If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer

and select **Tools > Internet Options**, click the **Connections** tab, and select the **Never dial a connection**. Other browsers provide similar options.

Changes Are Not Saved

If the router does not save the changes that you make on the router web pages, 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 computer or mobile device that you are using find your WiFi network? If not, check the WiFi LED on the front of the router. If it is off, you can press the **WiFi On/Off** button on the router to turn the router WiFi radios back on. 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 computer or mobile device support the security that you are using for your WiFi network (WPA or WPA2)?
- If you want to view the WiFi settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, and select **BASIC > Wireless**.

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

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

- Is your router too far from your device or too close? Place your device near the router but at least 6 feet (1.8 meters) away and see whether the signal strength improves.
- Are objects between the router and your computer or mobile device blocking the WiFi signal?

Troubleshoot Your Network Using the Ping Utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a network using the ping utility in your computer or workstation.

Test the 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 present:

- 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 Your Computer to a Remote Device

To test the path from your 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 131.

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](#)
- [Technical Specifications](#)

Factory Settings

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

For more information about resetting the router to its factory settings, see [Return the Router to Its Factory Default Settings](#) on page 96.

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

Table 4. Router factory default settings

Feature	Default Setting
Router login	
User login URL	www.routerlogin.net (or www.routerlogin.com or 192.168.1.1)
User name (case-sensitive)	admin
Default 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 39)
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 4. Router factory default settings (Continued)

Feature	Default Setting
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
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.
Operating mode	Up to 300 Mbps at 2.4 GHz Up to 433 Mbps at 5 GHz
Transmit power	100%, nonconfigurable
Guest WiFi network	
WiFi communication	Disabled
SSID name	2.4 GHz band: NETGEAR_Guest 5 GHz band: NETGEAR-5G_Guest
Security	None (open network)

Table 4. Router factory default settings (Continued)

Feature	Default Setting
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 5. Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, UPnP, and SMB
Power adapter	North America: 120V, 60 Hz, input All regions: 12V @ 1.0A output
Dimensions	Dimensions: 173 x 142 x 39 mm (6.8 x 5.5 x 1.5 in.)
Weight	Weight: 250 g (0.55 lbs)
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 10/100BASE-T
WAN	One RJ-45 port supporting 10/100BASE-T
WiFi	Maximum WiFi signal rate complies with the IEEE 802.11 standard. Note that the maximum wireless signal rate is derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.
Radio data rates	Auto-rate sensing
Data encoding standards	IEEE 802.11 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 5. Router specifications (Continued)

Feature	Description
Operating frequency range	2.4 GHz band <ul style="list-style-type: none"> • US: 2.412-2.462 GHz • Europe: 2.412-2.472 GHz • Australia: 2.412-2.472 GHz • China: 2.412-2.472 GHz 5 GHz band <ul style="list-style-type: none"> • 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 • China: 5.18-5.24 + 5.745-5.825 GHz
802.11 security	WPA2-PSK, WPA-PSK, WPA/WPA2 (mixed mode), and WEP