NETGEAR®

User Manual

Nighthawk WiFi 7 Tri-Band Router

Model RS300 and Model RS280

May 2024
202-12707-01

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

Support and Community

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

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

Regulatory and Legal

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

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

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

See the regulatory compliance document before connecting the power supply.

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

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

Do not use this device outdoors.

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

Trademarks

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

Revision History

Publication Part Number	Publish Date	Comments
202-12707-01	May 2024	First publication.

Contents

Chapter 1 Introduction

What is WiFi 7?..... 11
Additional documentation..... 11

Chapter 2 Hardware Setup

Unpack your router..... 13
Front panel LEDs and buttons..... 13
Rear panel..... 16
Router label..... 17
Position your router..... 18
Cable your router..... 19

Chapter 3 Connect to the Router Network and Access the Router

Connect to the router network..... 22
Connect to the router WiFi network..... 22
Connect to the router using a wired connection..... 22
Types of logins..... 23
Use a web browser to access the router..... 23
Automatic Internet setup..... 23
Log in to the router after you set up the router..... 25
Change the language..... 26
Install and manage your router with the Nighthawk app..... 26

Chapter 4 Specify Your Internet Settings

Use the Setup Wizard..... 29
Manually set up the Internet connection..... 30
Set an Internet connection without a login..... 30
Set a PPPoE Internet connection..... 32
Set a PPTP or L2TP Internet connection..... 33
About high-speed Internet connections and Internet port aggregation..... 35
Get multi-gigabit Internet with Internet port aggregation..... 36
Set an IPv6 Internet connection..... 37
Types of IPv6 Internet connections..... 37
Requirements for entering IPv6 addresses..... 38
Use auto detect for an IPv6 Internet connection..... 38
Set a 6to4 tunnel IPv6 Internet connection..... 39
Set a pass-through IPv6 Internet connection..... 41
Set a fixed IPv6 Internet connection..... 42

Set a DHCP IPv6 Internet connection..... 43
Set a PPPoE IPv6 Internet connection..... 45
Use auto config for an IPv6 Internet connection..... 47
Set a 6rd IPv6 Internet connection..... 48
Manage the MTU size..... 50
MTU concepts..... 50
Change the MTU size..... 51

Chapter 5 Control Access to the Internet

NETGEAR Armor..... 54
Activate Armor using the Nighthawk app..... 54
Network access control list..... 54
Enable the network access control list, set the access rule, and allow or block connected devices..... 55
Manage allowed devices currently not on the network..... 57
Manage blocked devices currently not on the network..... 59
Block Internet sites and services..... 60
Use keywords to block Internet sites..... 60
Delete keywords from the blocked list..... 62
Prevent blocking on a trusted computer..... 62
Block services from the Internet..... 63
Schedule when to block Internet sites and services..... 64
Set up security event email notifications..... 65

Chapter 6 Manage WiFi Settings

Change your country or region..... 68
Disable or reenable Smart Connect..... 68
Hide or broadcast the SSID for a WiFi network..... 69
Enable or disable 20/40 MHz coexistence for the 2.4 GHz radio. 70
Change the name for a WiFi network..... 71
Change the WiFi password or the WiFi security..... 71
Change the 2.4 GHz, 5 GHz, or 6 GHz WiFi channel..... 73
Change the WiFi mode..... 74
Set up a guest WiFi network..... 75
Manage advanced WiFi settings..... 77
Set up a WiFi schedule..... 77
Enable or disable MU-MIMO..... 78
Change the fragmentation length, CTS/RTS threshold, or preamble mode for a radio..... 79
Use the WPS Wizard for WiFi connections..... 80
Use the WPS Wizard with the push button..... 81
Use the WPS Wizard with a PIN..... 81

Chapter 7 Manage the WAN and LAN Network Settings

Manage the WAN settings..... 84
Change the WAN security settings..... 84
Set up a default DMZ server..... 85
Manage IGMP proxying..... 86
Manage NAT filtering..... 86
Manage the SIP application-level gateway..... 87
Change the LAN IP address settings or RIP settings..... 88
Set the IP addresses that the router assigns..... 89
Disable the DHCP server feature in the router..... 90
Manage reserved LAN IP addresses..... 91
Reserve an IP address..... 91
Edit a reserved IP address..... 92
Delete a reserved IP address entry..... 93
Manage custom static routes..... 93
Set up a static route..... 94
Edit a static route..... 95
Delete a static route..... 96
Set up an IPTV port or a bridge for a port group or VLAN tag group..... 96
Set up a bridge for a port group..... 97
Set up a bridge for a VLAN tag group..... 98
Manage Ethernet LAN port aggregation to a LAN device..... 99
Set up LAN port aggregation to a LAN device..... 100
View or change the router LAN port aggregation mode..... 101

Chapter 8 Optimize Performance

Enable QoS..... 104
Set the Internet bandwidth for your router..... 104
Update the QoS database..... 105
Manage Wi-Fi Multimedia QoS..... 106
Improve network connections with Universal Plug and Play..... 107

Chapter 9 Manage and Monitor Your Router

Update the router firmware..... 110
Check for new firmware and update the router..... 110
Manually upload firmware to the router 111
Manage the firmware update settings..... 112
Change the admin password..... 112
Enable admin password reset..... 113
Reset the admin password..... 114
Use HTTPS to access the router..... 115
Change the router’s device name..... 115

Manage the router configuration file..... 116
Back up the settings..... 116
Restore the settings..... 117
Erase the settings..... 117
Monitor the router and network..... 118
View information about the router and the Internet and WiFi settings..... 118
View devices currently on the network..... 119
View and manage logs of router activity..... 120
View the Internet connection status or renew the connection. 121
View the PPPoE Internet connection status or renew the connection..... 123
View the packet statistics of the Internet and LAN ports and WiFi networks 123
Monitor, meter, and control Internet traffic..... 124
Start the traffic meter without traffic volume restrictions..... 125
Restrict Internet traffic by volume..... 125
Restrict Internet traffic by connection time..... 127
View the Internet traffic volume and statistics..... 128
Unblock the traffic meter after the traffic limit is reached..... 128
Set the NTP server..... 129
Set your time zone and daylight saving time..... 130
Set up the router as a WiFi access point..... 131
Return the router to router mode..... 132
Manage LED blinking or turn off LEDs..... 132
Connect to your router with Anywhere Access..... 133
Return the router to its factory default settings..... 134
Use the Reset button..... 134
Erase the settings..... 135

Chapter 10 Share a USB Storage Device Attached to the Router

USB device requirements..... 137
Connect a USB storage device to the router..... 137
Display network folders on a storage device..... 138
Access a storage device connected to the router..... 139
Access a storage device connected to the router from a Windows-based computer..... 139
Map a USB device to a Windows network drive..... 139
Access a storage device connected to the router from a Mac. 140
Manage access to a USB storage device..... 141
Enable FTP access within your network..... 143
Change a network folder on a USB storage device..... 144
Add a network folder on a USB storage device..... 145
Safely remove a USB storage device..... 146

Change the media server settings or rescan media files..... 146

Chapter 11 Use Dynamic DNS to Access a USB Storage Device From the Internet

Set up and manage Dynamic DNS..... 149
Set up a new Dynamic DNS account..... 149
Use a Dynamic DNS account that you already have..... 150
Manage your existing NETGEAR or No-IP Dynamic DNS account..... 151
Your personal FTP server..... 152
Set up your personal FTP server: Overview of steps..... 152
Set up FTP access through the Internet..... 152
Set up HTTPS access through the Internet..... 153
Access a USB storage device through the Internet..... 154

Chapter 12 Use OpenVPN to Access Your Network

About VPN connections..... 157
LAN IP addressing in VPN networks..... 157
Enable OpenVPN service on the router..... 158
Install OpenVPN software on a VPN client..... 159
Install OpenVPN software on a Windows-based computer.. 160
Install OpenVPN software on a Mac..... 161
Install OpenVPN software on an iOS device..... 162
Install OpenVPN software on an Android device..... 163
Use VPN to access your Internet service at home..... 164
Allow VPN client Internet access in the router..... 164
Block VPN client Internet access in the router..... 165

Chapter 13 Manage Port Forwarding and Port Triggering

Manage port forwarding to a local server..... 168
Forward incoming traffic to a local server..... 168
Add a custom port forwarding service or application..... 169
Change a port forwarding rule..... 170
Remove a port forwarding rule..... 171
Application example: Make a local web server public..... 171
How the router implements the port forwarding rule..... 172
Manage port triggering..... 172
Add a port triggering rule..... 173
Change a port triggering rule..... 174
Remove a port triggering rule..... 175
Set the time-out period for port triggering..... 176
Disable an individual port triggering rule..... 176
Disable port triggering..... 177
Application example: Port triggering for Internet Relay Chat. 178

Chapter 14 Troubleshooting

Quick tips..... 180
Sequence to restart your network..... 180
Check the power adapter and Ethernet cable connections.. 180
Check the WiFi settings..... 180
Check the network settings..... 181
Reboot the router from its router web interface..... 181
Troubleshoot with the LEDs..... 182
Standard LED behavior when the router is powered on..... 182
Power LED is off 182
Power LED stays solid amber or blinking amber..... 182
Internet or Ethernet LAN port LEDs are off..... 183
WiFi LED is off..... 183
You cannot log in to the router..... 183
You cannot access the Internet..... 185
Troubleshoot Internet browsing..... 187
Changes are not saved..... 187
Troubleshoot WiFi connectivity..... 187
Troubleshoot your network using the ping utility..... 188
Test the LAN path to your router..... 188
Test the path from a Windows-based computer to a remote device..... 189

1

Introduction

This user manual is for the NETGEAR Nighthawk® WiFi 7 Tri-Band Router Model RS300 and Model RS280.

Model RS300 supports WiFi 7 (IEEE 802.11be) with a combined WiFi speed of up to 9.3 Gbps and tri-band concurrent radio operation:

- **2.4 GHz radio**: Supports IEEE 802.11 n/ac/ax/be with 4096-QAM, 20/40 MHz channel width, and a speed of up to 0.7 Gbps
- **5 GHz radio**: Support IEEE 802.11 n/ac/ax/be with 4096-QAM, 20/40/80/160 MHz channel width, and a speed of up to 2.9 Gbps
- **6 GHz radio**: Supports IEEE 802.11 ax/be with 4096-QAM, 20/40/80/160/320 MHz channel width, and a speed of up to 5.8 Gbps

Model RS280 supports WiFi 7 (IEEE 802.11be) with a combined WiFi speed of up to 9.2 Gbps and tri-band concurrent radio operation:

- **2.4 GHz radio**: Supports IEEE 802.11 n/ac/ax/be with 1024-QAM, 20/40 MHz channel width, and a speed of up to 0.6 Gbps
- **5 GHz radio**: Support IEEE 802.11 n/ac/ax/be with 4096-QAM, 20/40/80/160 MHz channel width, and a speed of up to 2.9 Gbps
- **6 GHz radio**: Supports IEEE 802.11 ax/be with 4096-QAM, 20/40/80/160/320 MHz channel width, and a speed of up to 5.8 Gbps

Both routers provide one 2.5GbE Internet port for cable and fiber ISP connections up to 2.5 Gbps, two 2.5GbE LAN ports for connection to high-speed LAN devices, and two 1 Gigabit LAN ports.

This chapter contains the following sections:

- What is WiFi 7?
- Additional documentation

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

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

NOTE: In this manual, *WiFi network* means the same thing as SSID (service set identifier or WiFi network name) or VAP (virtual access point). That is, when we refer to a WiFi network we mean an individual SSID or VAP.

What is WiFi 7?

WiFi 7, also known as IEEE 802.11be Extremely High Throughput (EHT), is a next-generation WiFi standard. The new standard provides the capability for multi-gigabit (multi-gig) WiFi throughout the home with faster speeds, less interference, and better performance for high-bandwidth online activities.

New technologies in WiFi 7 provide the following benefits:

- 2.4 times faster speed than WiFi 6
- Double the maximum bandwidth for your devices
- Lower latency than WiFi6
- A more reliable connection

For more information, visit the NETGEAR WiFi 7 page at netgear.com/home/discover/wifi7.

Additional documentation

The following documents are available at netgear.com/support/download/:

- Quick start guide
- Data sheet

For information about the NETGEAR Nighthawk app, visit netgear.com/home/services/nighthawk-app/.

2

Hardware Setup

This chapter contains the following sections:

- Unpack your router
- Front panel LEDs and buttons
- Rear panel
- Router label
- Position your router
- Cable your router

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

Unpack your router

Your package contains the router, an Ethernet cable, and the power adapter (the type varies by region).

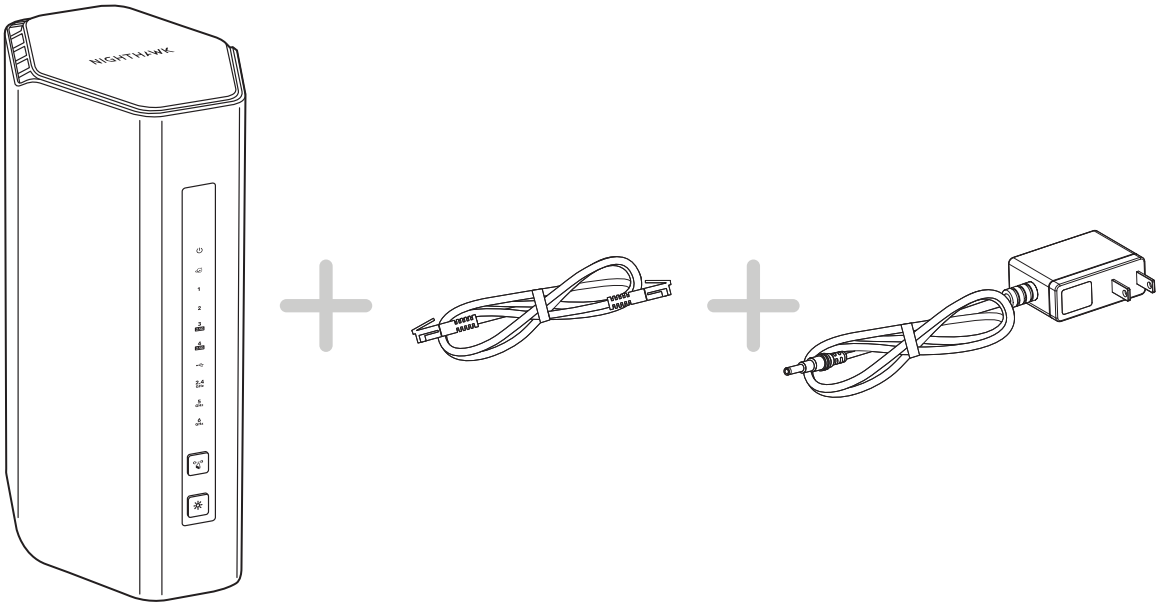

Figure 1. Package contents

Front panel LEDs and buttons

The status LEDs and two buttons are located on the front panel of the router.

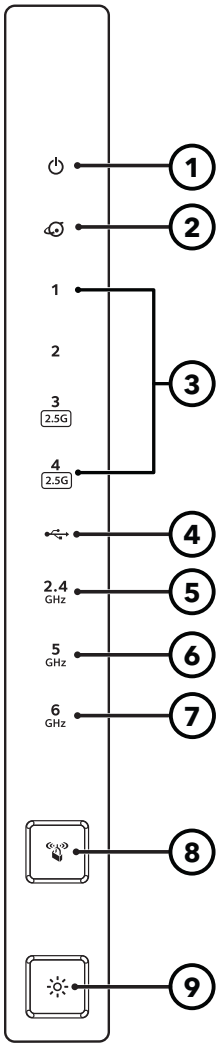

Figure 2. Top view

Table 1. LED descriptions

LED and Button	Description
1. Power LED	**Solid white**: The router is ready. **Solid amber and then blinking amber**: The **Reset** button was pressed. When you first press the **Reset** button, the LED lights solid amber. After 5 seconds, the LED turns blinking amber, and the router resets to factory defaults. **Off**: Power is not supplied to the router.
2. Internet LED	**Solid white**: The Internet connection is ready. **Solid amber**: A cable was plugged into the port, but the Internet connection is not yet ready. **Blinking**: The port is sending or receiving traffic. **Off**: No Ethernet cable is connected between the router and the modem.

Table 1. LED descriptions (Continued)

LED and Button	Description
3. Ethernet LAN ports 1–4 LEDs 1 2 3 2.5G 4 2.5G	The LED color indicates the speed of the Ethernet connection at each LAN port: white for the maximum supported speed on each port (1 Gbps on ports 1-2, 2.5 Gbps on ports 3-4) and amber for lower speeds. **Solid white**: The router detected a 1 Gbps (ports 1-2) or 2.5 Gbps (ports 3-4) link with a powered-on device. **Blinking white**: The port is sending or receiving traffic at 1 Gbps (ports 1-2) or 2.5 Gbps (ports 3-4). **Solid amber**: The router detected a lower speed link with a powered-on device. **Blinking amber**: The port is sending or receiving traffic at a lower speed. **Off**: No device is connected to this Ethernet LAN port.
4. USB 3.0 port LED	**Solid white**: A USB device is connected to the USB 3.0. port. **Blinking white**: The USB 3.0 port is sending or receiving traffic. **Off**: No USB device is connected to the USB 3.0 port.
5. 2.4 GHz WiFi LED 2.4 GHz	**Solid white**: The 2.4 GHz WiFi radio is operating. **Off**: The 2.4 GHz WiFi radio is off.
6. 5 GHz WiFi LED 5 GHz	**Solid white**: The 5 GHz WiFi radio is operating. **Off**: The 5 GHz WiFi radio is off.
7. 6 GHz WiFi LED 6 GHz	**Solid white**: The 6 GHz WiFi radio is operating. **Off**: The 6 GHz WiFi radio is off.
8. Sync/WPS LED	Pressing the **Sync/WPS** button lets your WPS-enabled device join your router's WiFi network without typing the WiFi password. **Solid white**: The Sync/WPS LED is always solid white. This is normal behavior. **Blinking white**: The WPS process is active so that you can connect a WPS-enabled device to your router's WiFi network. When the device is connected, the sync/WPS LED shows solid white again. The Sync/WPS LED is also blinking white when the router is in factory default state or you reset the router to factory default settings. **Off**: The router or its LEDs are turned off.
9. LED On/Off button	Pressing the **LED On/Off** button turns off all LEDs except for the Power LED.

Rear panel

The following figure shows the rear panel connectors and buttons.

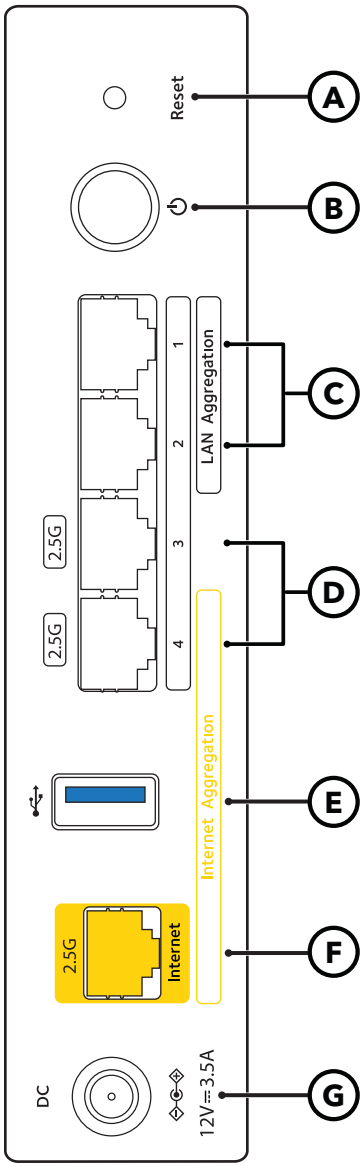

Figure 3. Rear panel

The rear panel contains the following components:

- **A. Reset button**: Pressing the **Reset** button resets the router.

  If the **Reset** button is pressed for at least five seconds and the Power LED blinks amber, the router returns to its factory settings.
- **B. Power On/Off button**: Press the **Power On/Off** button to provide power to the router.

- **C. Gigabit Ethernet LAN ports**: Two Gigabit Ethernet RJ-45 LAN ports that support 1G, 100M, and 10M speed. Use these ports to connect Ethernet LAN devices to your router.
  The router supports port aggregation:
  - **LAN aggregation**: Use Ethernet LAN ports 1 and 2 to set up a port aggregation link to a LAN device that also supports Ethernet LAN port aggregation. For more information, see Manage Ethernet LAN port aggregation to a LAN device on page 99.
- **D. 2.5G LAN ports**: Two RJ-45 LAN ports that support speeds up to 2.5 Gbps. Use a Category 5e (Cat5e) Ethernet cable or higher rated Ethernet cable to connect the router to a high-speed LAN server, LAN storage device, or another LAN device.
  The router supports port aggregation:
  - **Internet (WAN) aggregation**: Use Ethernet LAN port 4 with the 2.5G Internet port to set up a multi-gigabit Internet connection with port aggregation. For more information, see Get multi-gigabit Internet with Internet port aggregation on page 36.

  NOTE: You can set up both LAN aggregation and Internet (WAN) aggregation.
- **E. USB 3.0 port**: Use the USB 3.0 port to connect a USB storage device to your router.
- **F. 2.5G Internet port**: An RJ-45 Internet port (marked with yellow) that supports speeds up to 2.5 Gbps. Use a Category 5e (Cat5e) Ethernet cable or higher rated Ethernet cable to connect a high-speed modem for a high-speed Internet connection. For more information, see About high-speed Internet connections and Internet port aggregation on page 35.
- **G. DC power connector**: Connect the power adapter that came in your product package to the DC power connector.

Router label

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

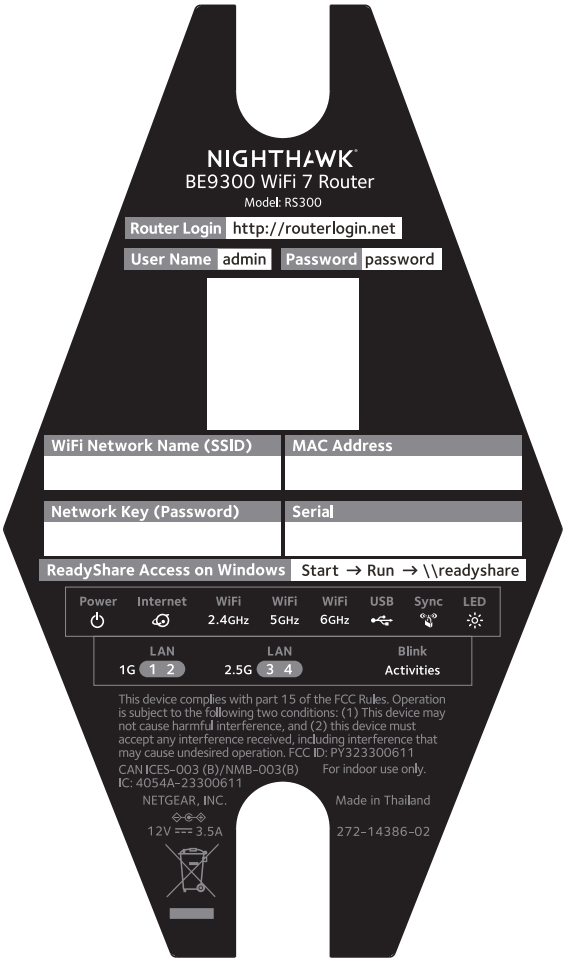

Figure 4. Router label

Position your router

The router lets you access your network anywhere within the operating range of your WiFi network. However, the operating distance or range of your WiFi connection can vary significantly depending on the physical placement of your router.
In addition, position your router according to the following guidelines:

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

- To avoid wireless signal interference, place the router away from electrical devices such as these:
  - Ceiling fans
  - Home security systems
  - Microwaves
  - Computers
  - The base of a cordless phone
  - 2.4 GHz or 5 GHz cordless phones
- Place the router away from large metal surfaces, large glass surfaces, insulated walls, and items such as these:
  - Solid metal doors
  - Aluminum studs
  - Fish tanks
  - Mirrors
  - Brick
  - Concrete

The following factors might limit the range of your WiFi:

- The thickness and number of walls the WiFi signal passes through can limit the range.
- 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 devices that emit a WiFi signal for network access.

Cable your router

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

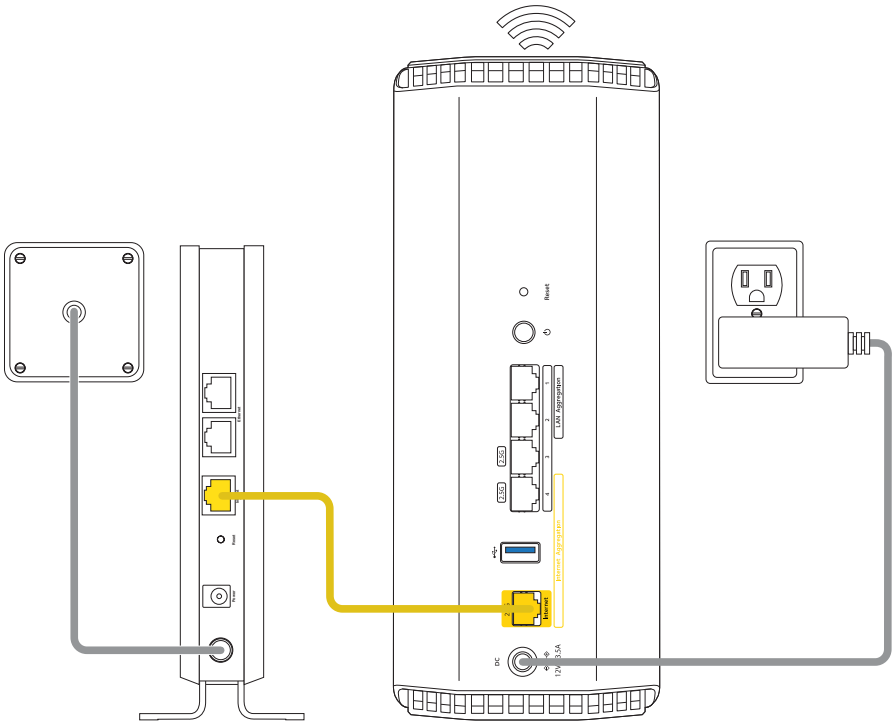

Figure 5. Cable your router

To cable your router:

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

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

3. Connect the power adapter to your router and plug the power adapter into an outlet.

   The router's Power LED lights solid white when the router is ready.

After you connect your router to a modem and power it on, finish your router's installation process using the Nighthawk app or router web interface. For more information, see Connect to the Router Network and Access the Router on page 21.

3

Connect to the Router Network and Access the Router

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

The chapter contains the following sections:

- Connect to the router network
- Types of logins
- Use a web browser to access the router
- Install and manage your router with the Nighthawk app

Connect to the router network

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

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

Connect to the router WiFi network

You can connect a WiFi-enabled computer or mobile device to the router WiFi network using the router WiFi network name (SSID) and WiFi password (network key)

To connect to the WiFi network:

1. Make sure that the router is receiving power (its Power LED is lit).
2. On your computer or mobile device, open your WiFi network management application.

   This is the application that lets you manage your WiFi connections.
3. Find and select the router WiFi network name (SSID).

   The router's default WiFi network name (SSID) is on the router label.
4. Enter the router WiFi password.

   The router's default WiFi password is on the router label. The WiFi password is also known as the network key or passphrase.

   Your computer or mobile device connects to the WiFi network.

Connect to the router using a wired connection

You can connect your computer to the router using an Ethernet cable and join the router's local area network (LAN). After setup, you can also connect other wired devices.

To connect your computer or other device 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.

   If your computer doesn't have an Ethernet port, you might be able to connect a USB to Ethernet adapter to a USB port on your computer, and then connect the Ethernet cable to the adapter's port.
3. Connect the other end of the Ethernet cable to an Ethernet LAN port on the router.

Your computer connects to the local area network (LAN).

Types of logins

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

Several types of logins are associated with the router:

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

Use a web browser to access the router

When you connect to the network (either with WiFi or with an Ethernet cable), you can use a web browser to access the router to view or change its settings. We call the router user interface the *router web interface*.

When you access the router web interface, 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 (see the information below) or manually (see Manually set up the Internet connection on page 30). In either case, you must use a web browser to access the router.

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 example, 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.

NOTE: If your Internet service is going through your TV or fiber cable, you might not need the login information.

When your Internet connection is working, you no longer need to launch the ISP login program on your computer to access the Internet. When you start an Internet application, your router automatically logs you in.

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

To automatically set up your router:

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

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

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

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

   The page that displays recommends that you use the Nighthawk app. However, the current procedure describes how you can use the router web interface.
4. If the installation process does not start and the browser does not display the page that recommends that you use the Nighthawk app, do the following:

- Make sure that the computer is connected to one of the Ethernet LAN ports on the router 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.
- Use the **Reset** button, to reset the router to factory default settings (see Use the Reset button on page 134).

5. Scroll down and click the **If you don't have a compatible smartphone, click here** link.

   A welcome page displays.
6. Follow the onscreen instructions.

   The router detects your Internet settings.
7. Follow the onscreen instructions to complete the installation process.

If the router does not detect the Internet settings, the installation assistant cannot complete the installation process, and you must start the installation process again:

1. Before you start again, review your settings. Make sure that you select the correct options and type everything correctly.
2. If the router still does not detect the Internet settings, contact your ISP to verify that you are using the correct configuration information.
3. If problems persist, register your router and contact NETGEAR Technical Support.

Log in to the router after you set up the router

When you set up your router while the router is in factory default state, the browser automatically starts the NETGEAR installation assistant.

After you set up the router, if you want to view or change settings for the router, you can use a browser to log in to the router web interface.

To log in to the router web interface:

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

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

A login window opens.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

Change the language

By default, the Auto setting uses your region to automatically set the language that displays when you log in to the router web interface.

To change the language:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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.

Install and manage your router with the Nighthawk app

With the Nighthawk app, you can easily install and manage your router. The app lets you update the router to the latest firmware, allows you to personalize your WiFi network, and helps you to register your router with NETGEAR. You can also manage your router remotely and use the Armor and Smart Parental Controls services.

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

NOTE: Your router is not connected to the Internet until you finish setting it up with the app. If you are connected to your router's WiFi network before your router is set up, you do not have Internet access and cannot download the app.

Use your cellular data or connect to your previous router's WiFi network to download the app. During router installation, the app instructs you when you need to connect to your router's WiFi.

To install your router using the Nighthawk app:

1. Visit Nighthawk-app.com to download the Nighthawk app.

   NOTE: To download the app, you need to use your cellular data or connect your mobile device to your previous router's WiFi network.

2. Wait for the Nighthawk app to download on your mobile device.
3. Launch the Nighthawk app.
4. Follow the instructions that display in the app to install your router and connect to the Internet.

4

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.

After you set up your router, you can use the Setup Wizard to redetect the Internet settings, or you can manually specify your Internet settings.

This chapter contains the following sections:

- Use the Setup Wizard
- Manually set up the Internet connection
- Set an IPv6 Internet connection
- Manage the MTU size

Use the Setup Wizard

You can use the Setup Wizard to redetect your Internet settings and automatically set up your router.

To use the Setup Wizard:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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.
6. Click the **Next** button.

   The Setup Wizard searches your Internet connection for servers and protocols to determine your Internet configuration.
7. Follow the onscreen instructions.

   The router detects your Internet settings.
8. Follow the onscreen instructions to complete the Setup Wizard process.

If the router does not detect the Internet settings, the Setup Wizard cannot complete its process, and you must start the Setup Wizard again:

1. Before you start again, review your settings. Make sure that you select the correct options and type everything correctly.
2. If the router still does not detect the Internet settings, contact your ISP to verify that you are using the correct configuration information.
3. If problems persist, register your router and contact NETGEAR Technical Support.

Manually set up the Internet connection

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

Set 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 set an Internet connection without a login:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Internet Setup page displays.
5. In the **WAN Preference** section, select one of the following options:
   - **Internet Port (2.5 Gbps)**. Select this option if you connected a modem to the Internet port on your router. For more information about a high-speed Internet connection, see About high-speed Internet connections and Internet port aggregation on page 35.
   - **Multi-Gig Internet (2.5 Gbps + 2.5 Gbps)**. Select this option if you want to set up multi-gigabit Internet and use the Internet port together with Ethernet LAN port 4 for your Internet connection. For more information, see Get multi-gigabit Internet with Internet port aggregation on page 36.
6. In the Does your Internet connection require a login? section, leave the **No** radio button selected.
7. If your Internet connection requires an account name or host name, do the following:

a. In the Account Name section, click the **Edit** button.
b. Enter the account name.

   By default, the account name is the model number of the router.
c. Click the **Apply** button.
d. Select **Internet**.

   The Internet Setup page displays again.

8. 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.
9. 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.
10. 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.
11. 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.
12. Click the **Apply** button.

    Your settings are saved.
13. Click the **Test** button to test your Internet connection.

    If the NETGEAR website does not display within one minute, see You cannot access the Internet on page 185.

Set a PPPoE Internet connection

You can manually set 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 set a PPPoE Internet connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Internet Setup page displays.
5. In the **WAN Preference** section, select one of the following options:
   - **Internet Port (2.5 Gbps)**. Select this option if you connected a modem to the Internet port on your router. For more information about a high-speed Internet connection, see About high-speed Internet connections and Internet port aggregation on page 35.
   - **Multi-Gig Internet (2.5 Gbps + 2.5 Gbps)**. Select this option if you want to set up multi-gigabit Internet and use the Internet port together with Ethernet LAN port 4 for your Internet connection. For more information, see Get multi-gigabit Internet with Internet port aggregation on page 36.
6. In the Does your Internet connection require a login? section, select the **Yes** radio button.

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

   This is the default selection in the menu.
8. In the **Login** field, enter the login name that your ISP gave you.

   This login name is often an email address.
9. In the **Password** field, type the password that you use to log in to your Internet service.
10. If your ISP requires a service name, type it in the **Service Name (if Required)** field.

11. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.
12. 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.
13. 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.
14. 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.
15. 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.
16. Click the **Apply** button.

    Your settings are saved.
17. Click the **Test** button to test your Internet connection.

    If the NETGEAR website does not display within one minute, see You cannot access the Internet on page 185.

Set a PPTP or L2TP Internet connection

You can manually specify the connection settings for a PPTP or L2TP Internet service for which you must log in. Use the information that your 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 set a PPTP or L2TP Internet connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Internet Setup page displays.
5. In the **WAN Preference** section, select one of the following options:
   - **Internet Port (2.5 Gbps)**. Select this option if you connected a modem to the Internet port on your router. For more information about a high-speed Internet connection, see About high-speed Internet connections and Internet port aggregation on page 35.
   - **Multi-Gig Internet (2.5 Gbps + 2.5 Gbps)**. Select this option if you want to set up multi-gigabit Internet and use the Internet port together with Ethernet LAN port 4 for your Internet connection. For more information, see Get multi-gigabit Internet with Internet port aggregation on page 36.
6. Select the Does your Internet connection require a login? **Yes** radio button.

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

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

   This login name is often an email address.
9. In the **Password** field, type the password that you use to log in to your Internet service.
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. If your ISP gave you fixed IP addresses and a connection ID or name, type them in the **My IP Address**, **Subnet Mask**, **Server Address**, **Gateway IP Address**, and **Connection ID/Name** fields.

    If your ISP did not give you IP addresses, a connection ID, or name, leave these fields blank. The connection ID or name applies to a PPTP service only.

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 185.

About high-speed Internet connections and Internet port aggregation

Use the router's yellow Internet port, which supports speeds up to 2.5 Gbps, to connect the router to your modem.

The router's Internet speed depends on the speed that your ISP offers and the speed that your modem supports. For example, if your ISP and your modem both support a speed of 2.5 Gbps, the router's Internet speed is also 2.5 Gbps. However, if, for example, your ISP supports a speed of 2.5 Gbps but your modem supports a speed of only 1 Gbps, your router's Internet speed is limited to 1 Gbps.

If your ISP offers Internet speeds faster than 2.5 Gbps, your modem does *not* provide a high-speed or multi-gigabit port, but your modem does support link aggregation, set up Internet port aggregation by aggregating the yellow Internet port and Ethernet LAN

port 4 on the router. By default, the Ethernet LAN 4 port functions as a regular LAN port, but you change the function of the Ethernet LAN port 4 to a second WAN port in an Internet link aggregation setup. For more information, see Get multi-gigabit Internet with Internet port aggregation on page 36.

Get multi-gigabit Internet with Internet port aggregation

If your ISP offers Internet speeds faster than 1 Gbps, your modem does *not* provide a high-speed or multi-gigabit port, but your modem does support link aggregation, you can get multi-gigabit Internet with your router by setting up Internet port aggregation. You can aggregate the Internet port and Ethernet LAN port 4 on the router.

NOTE: For information about a different type of aggregation, which is port aggregation to a *LAN* device, see Manage Ethernet LAN port aggregation to a LAN device on page 99.

To set up Internet port aggregation, you need the following:

- A service provider that offers an Internet speed that's over 1 Gbps.
- A modem that support both an Internet speed that's over 1 Gbps and two Ethernet ports that support static Link Aggregation Control Protocol (LACP), for example, the NETGEAR Nighthawk Multi-Gig Cable Modem, model CM1200.

To set up Internet port aggregation:

1. Set up Internet port aggregation on your modem.

   For information about how to set up Internet port aggregation on your modem, see the documentation that came with your modem.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Internet Setup page displays.
6. In the **WAN Preference** section, select the **Multi-Gig Internet (2.5 Gbps + 2.5 Gbps)** radio button.

7. Click the **Apply** button.

   Your settings are saved.
8. Connect the yellow Internet port and the Ethernet LAN port 4 on your router to two Ethernet ports on your modem.

Set an IPv6 Internet connection

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

Types of IPv6 Internet connections

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

- **Auto Detect**: See Use auto detect for an IPv6 Internet connection on page 38.
- **6to4 tunnel**: See Set a 6to4 tunnel IPv6 Internet connection on page 39.
- **Pass-through**: See Set a pass-through IPv6 Internet connection on page 41.
- **Fixed**: See Set a fixed IPv6 Internet connection on page 42.
- **DHCP**: See Set a DHCP IPv6 Internet connection on page 43.
- **PPPoE**: See Set a PPPoE IPv6 Internet connection on page 45.
- **Auto Config**: See Use auto config for an IPv6 Internet connection on page 47.
- **6rd**: See Set a 6rd IPv6 Internet connection on page 48.

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

- 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 38).
- If your ISP did not provide details, use the 6to4 tunnel connection type (see Set a 6to4 tunnel IPv6 Internet connection on page 39).

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 router does not expect to receive such a packet, or the packet is not in the connection record, the router blocks this packet.

Requirements for entering IPv6 addresses

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

All of the following examples specify the *same* IPv6 address:

- 2001:db8:0000:0000:020f:24ff:febf:dbcb
- 2001:db8:0:0:20f:24ff:febf:dbcb
- 2001:db8::20f:24ff:febf:dbcb
- 2001:db8:0:0:20f:24ff:128.141.49.32

The following errors invalidate an IPv6 address:

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

Use auto detect for an IPv6 Internet connection

To set up an IPv6 Internet connection through autodetection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

   The page adjusts.

   After you click the Apply button, 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. However, not every IPv6 connection type shows the WAN address information.
- **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**: Use this method if devices on the LAN cannot receive an IPv6 address through auto configuration but must receive the IPv6 address through a DHCP server.
   - **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 **Enable RIPng** check box.

   This selection enables RIP Next Generation (RIPng) on IPv6 Internet connections. RIPng is an extension of Routing Information Protocol (RIP) that supports IPv6. You might want to enable RIPng if you are an advanced user with a complex home network configuration that requires dynamic routing.

8. (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.

9. Click the **Apply** button.

   Your settings are saved.

Set a 6to4 tunnel IPv6 Internet connection

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

To set a 6to4 tunnel IPv6 Internet connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **6to4 Tunnel**.

   The page adjusts.

   After you click the Apply button, 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. This option uses the DNS servers assigned by the ISP for the IPv6 connection.
   - **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**: Use this method if devices on the LAN cannot receive an IPv6 address through auto configuration but must receive the IPv6 address through a DHCP server.
   - **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 a pass-through IPv6 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 a pass-through IPv6 Internet connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 a fixed IPv6 Internet connection

To set a fixed IPv6 Internet connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

   The page adjusts.
6. Configure the fixed IPv6 addresses for the WAN connection:

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

   NOTE: If you do not specify the DNS servers, the router uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup page. (See Manually set up the Internet connection on page 30.)
7. Select an IP Address Assignment radio button:

   - **Use DHCP Server**: Use this method if devices on the LAN cannot receive an IPv6 address through auto configuration but must receive an IPv6 address through a DHCP server.
   - **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. (Optional) Select the **Enable RIPng** check box.

This selection enables RIP Next Generation (RIPng) on IPv6 Internet connections. RIPng is an extension of Routing Information Protocol (RIP) that supports IPv6. You might want to enable RIPng if you are an advanced user with a complex home network configuration that requires dynamic routing.

9. 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.

10. Click the **Apply** button.

    Your settings are saved.

Set a DHCP IPv6 Internet connection

To set a DHCP IPv6 Internet connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

   The page adjusts.

   After you click the Apply button, the router automatically detects the information in the following fields:

   - **Router's IPv6 Address on WAN**: This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
   - **Router's IPv6 Address on LAN**: This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
6. (Optional) In the **User Class (If Required)** field, enter a host name.

Most people can leave this field blank, but if your ISP gave you a specific host name, enter it here.

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

   You can type the domain name of your IPv6 ISP. Do not enter the domain name for the IPv4 ISP here. 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**: Use this method if devices on the LAN cannot receive an IPv6 address through auto configuration but must receive an IPv6 address through a DHCP server.
   - **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 **Enable RIPng** check box.

    This selection enables RIP Next Generation (RIPng) on IPv6 Internet connections. RIPng is an extension of Routing Information Protocol (RIP) that supports IPv6. You might want to enable RIPng if you are an advanced user with a complex home network configuration that requires dynamic routing.

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.

Set a PPPoE IPv6 Internet connection

To set a PPPoE IPv6 Internet connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

   The page adjusts.

   After you click the Apply button, 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. Configure the login settings:

   a. In the **Login** field, enter the login information for the ISP connection.

      This is usually the name that you use in your email address. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.

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

   c. In the **Service Name** field, enter a service name.

      If your ISP did not provide a service name, leave this field blank.

NOTE: The default setting of the **Connection Mode** menu is Always On to provide a steady IPv6 connection. The router never terminates the connection. If the connection is terminated - for example, when the modem is turned off - the router attempts to reestablish the connection immediately after the PPPoE connection becomes available again.

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

   - **Get Automatically from ISP**: Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address. This option uses the DNS servers assigned by the ISP for the IPv4 connection.
   - **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**: Use this method if devices on the LAN cannot receive an IPv6 address through auto configuration but must receive the IPv6 address through a DHCP server.
   - **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 **Enable RIPng** check box.

   This selection enables RIP Next Generation (RIPng) on IPv6 Internet connections. RIPng is an extension of Routing Information Protocol (RIP) that supports IPv6.

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

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

11. Click the **Apply** button.

    Your settings are saved.

Use auto config for an IPv6 Internet connection

To set up an IPv6 Internet connection through auto configuration:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

   The page adjusts.

   After you click the Apply button, 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. Unless the ISP assigns DNS servers through DHCPv6, this option uses the DNS servers assigned by the ISP for the IPv4 connection.
- **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**: Use this method if devices on the LAN cannot receive an IPv6 address through auto configuration but must receive the IPv6 address through a DHCP server.
   - **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 **Enable RIPng** check box.

    This selection enables RIP Next Generation (RIPng) on IPv6 Internet connections. RIPng is an extension of Routing Information Protocol (RIP) that supports IPv6.
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.

Set a 6rd IPv6 Internet connection

The 6rd protocol makes it possible to deploy IPv6 to sites using a service provider's IPv4 network. 6rd uses the service provider's own IPv6 address prefix. This limits the operational domain of 6rd to the service provider's network and is under direct control of the service provider. The IPv6 service provided is equivalent to native IPv6. The 6rd mechanism relies on an algorithmic mapping between the IPv6 and IPv4 addresses that are assigned for use within the service provider's network. This mapping allows for automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, allowing stateless operation of 6rd.

With a 6rd tunnel configuration, the router follows the RFC5969 standard, supporting two ways to establish a 6rd tunnel IPv6 WAN connection:

- **Auto Detect mode**: In IPv6 Auto Detect mode, when the router receives option 212 from the DHCPv4 option, autodetect selects the IPv6 as 6rd tunnel setting. The router

uses the 6rd option information to establish the 6rd connection. For more information, see Use auto detect for an IPv6 Internet connection on page 38.

- **Manual mode**: In 6rd mode, if the router receives option 212, the fields are automatically completed. Otherwise, you must enter the 6rd settings.

To set a 6rd IPv6 Internet connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

   The page adjusts.

   After you click the Apply button, the router automatically detects the information in the following sections:

   - **6rd (IPv6 Rapid Development) Configuration**: The router detects the service provider's IPv4 network and attempts to establish an IPv6 6rd tunnel connection. If the IPv4 network returns 6rd parameters to the router, the page adjusts to display the correct settings in this section.
   - **Router's IPv6 Address on LAN**: This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.
6. If the router does not automatically detect the information in the 6rd fields, specify the following 6rd settings:
   - **6rd Prefix**: Type the IPv6 prefix that your ISP gave you.
   - **6rd Prefix Length**: Type the IPv6 prefix length that your ISP gave you.
   - **6rd IPv4 Border Relay Address**: Type the border router's IPv4 address that your ISP gave you.
   - **6rd IPv4 Address Mask Length**: Type the IPv4 mask length that your ISP gave you.
7. Select an IPv6 Domain Name Server (DNS) Address radio button:

- **Get Automatically from ISP**: Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address. This option uses the DNS servers assigned by the ISP for the IPv4 connection.
- **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**: Use this method if devices on the LAN cannot receive an IPv6 address through auto configuration but must receive the IPv6 address through a DHCP server.
   - **Auto Config**: This is the default setting.

   This setting specifies how the router assigns IPv6 addresses to the devices on your home network (the LAN).
9. (Optional) Select the **Use This Interface ID** check box and specify the interface ID that you want to be used for the IPv6 address of the router's LAN interface.

   If you do not specify an ID here, the router generates one automatically from its MAC address.
10. (Optional) In the **MTU Size (in bytes)** field, enter a size in bytes.

    The default size for this type of IPv6 connection is 1480 bytes.
11. Click the **Apply** button.

    Your settings are saved.

Manage the MTU size

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

MTU concepts

When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If a device in the data path uses a lower maximum transmission unit (MTU) setting than the other devices, the data packets must be split or "fragmented" to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

- You experience problems connecting to your Internet service, and the technical support of either the Internet service provider (ISP) or NETGEAR recommends changing the MTU setting.

  For example, if a secure website does not open, or displays only part of a web page, you might need to change the MTU.
- You use VPN and experience severe performance problems.
- You used a program to optimize MTU for performance reasons and now you are experiencing connectivity or performance problems.

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

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

Table 2. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1458	Used in PPPoA environments.
1436	Used in PPTP environments or with VPN.

Change the MTU size

To change the MTU size:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 616 to 1500.
6. Click the **Apply** button.

   Your settings are saved.

5

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 contains the following sections:

- NETGEAR Armor
- Activate Armor using the Nighthawk app
- Network access control list
- Block Internet sites and services
- Set up security event email notifications

NETGEAR Armor

Your router supports NETGEAR Armor.

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

NETGEAR Armor includes an anti-malware application for your Windows-based computers and your Mac OS, iOS, and Android devices.

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

You can use the Nighthawk app to view and manage NETGEAR Armor.

Activate Armor using the Nighthawk app

To activate Armor using the Nighthawk app:

1. Launch the Nighthawk app.

   The dashboard displays.
2. Tap **Security**.

   The Security page displays.

   If Armor was not yet activated, it is now activated automatically, or you are prompted to purchase Armor.

Network access control list

You can use the network access control list (ACL) on the router to block or allow access to your network and the Internet. The ACL identifies a WiFi or wired device by its MAC address. The router detects the MAC addresses of the devices on the network and either allows or denies access.

The router detects and stores the MAC addresses of devices that connect to the network, so it lists the MAC addresses both of devices that are currently connected and any that were previously connected.

If you set up a network ACL that *allows* all new devices to connect, the following applies:

- You can either select or manually enter devices that you want to *block* from connecting to the network.
- All other devices are allowed access to the network.

If you set up a network ACL that *blocks* all new devices from connecting, the following applies:

- You can either select or manually enter devices that you want to *allow* access to the network.
- Devices that are currently connected to the network or that were allowed to connect in the past are automatically placed on the network ACL as allowed devices.
- All other devices are denied access to the network.

NOTE: Each network device has a MAC address that serves as a unique identifier. The MAC address is a 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of a device. If you cannot see the label, you can display the MAC address using the network configuration utilities on your computer or mobile device.

Enable the network access control list, set the access rule, and allow or block connected devices

When you enable network access control, you must select whether new devices are automatically allowed to access the network or are blocked from accessing the network. By default, devices that are already connected to the network are added to the ACL as allowed, but you can choose to block one or more of these devices from accessing the network.

To enable and manage the network access control list for the entire network and allow or block connected devices:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 select an access rule and use the Allow and Block buttons. When the Turn on Access Control check box is cleared, all devices are allowed to connect, even if a device is on the list of blocked devices.
6. Select an access rule to apply to new devices:
   - **Allow all new devices to connect**: With this setting, if you connect a new device to the network, it can access the network. You do not need to enter its MAC address on this page. This option works for most home networks. You can also block one or more devices from accessing the network. For more information, see the following step.
   - **Block all new devices from connecting**: With this setting, if you want to allow a new device to connect, you must enter its MAC address on this page. (In this situation, a new device is a device that was not previously connected to the network.) For more information about allowing one or more devices, see the following step.

     If you block all *new* devices from connecting, the device that you are currently using to connect to the router web interface, any other devices that are currently connected to the network, and all devices that were allowed to connect to the network in the past *are* still allowed access. That means that these devices are automatically added to the network ACL as allowed devices. If you want to block any of these devices, see the following step.

   NOTE: Selecting an access rule does not affect previously blocked or allowed devices. It applies only to *new* devices trying to access the network after you apply this setting.
7. To change access for devices that are connected or were connected to the network, do the following:
   - **Currently connected devices**:

     In the table that contains the ACL, the Status column shows either Allowed or Blocked for a device. To change the status, select the check box for the device, and click either the **Allow** button or the **Block** button.

NOTE: If you blocked all new devices from connecting, make sure that the computer or mobile device that you are currently using to access the router web interface shows as Allowed in the Status column.

- **Devices that were connected in the past:**
  - To manage allowed devices that are currently not connected to the network, see Manage allowed devices currently not on the network on page 57.
  - To manage blocked devices that are currently not connected to the network, see Manage blocked devices currently not on the network on page 59.

8. Click the **Apply** button.

   Your settings are saved.

Manage allowed devices currently not on the network

If you set up an access control list (ACL) that blocks all new devices from accessing the network, you can add new devices that must be allowed access to the network, remove old devices, or change whether devices that were allowed must now be blocked when they try to connect to the network.

For example, you could add a second computer or mobile device for access to the router web management interface in case the device that you are currently using needs to be removed from the network for repairs.

To manage allowed devices currently not on the network:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Access Control page displays.
5. Click the **View list of allowed devices not currently connected to the network** link.

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

In the following steps, we refer to the list of allowed devices not currently connected to the network as *the list of allowed devices*.

6. To add a device to the list of allowed devices, do the following:
   a. Click the **Add** button.

      The Add Allowed Device page displays.
   b. Enter the MAC address and device name for the device that you want to allow.
   c. On the Add Allowed Device page, click the **Apply** button.

      The device is added to the list of allowed devices.
7. To remove a device from the list of allowed devices, do the following:
   a. Select the check box for the device.
   b. Click the **Remove from the list** button.

      The device is removed from the list of allowed devices.
8. To change the device status by blocking access for a device on the list of allowed devices, do the following:
   a. Select the check box for the device.
   b. Click the **Edit** button.

      The Edit Device Name page displays.
   c. From the **Access Control** menu, selected **Block**.
   d. On the Edit Device Name page, click the **Apply** button.

      The device is moved to the list of blocked devices not currently connected to the network.
9. To change the device name for a device on the list of allowed devices, do the following:
   a. Select the check box for the device.
   b. Click the **Edit** button.

      The Edit Device Name page displays.
   c. In the **Device Name** field, enter a name.
   d. On the Edit Device Name page, click the **Apply** button.

      The device name is changed on the list of allowed devices.
10. Click the **Apply** button.

    Your settings are saved.

Manage blocked devices currently not on the network

If you set up an access control list (ACL) that allows all new devices to access the network, you can add new devices that must be blocked from accessing the network, remove old devices, or change whether devices that were blocked must now be allowed when they try to connect to the network.

To manage blocked devices currently not on the network:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Access Control page displays.
5. Click the **View list of blocked devices not currently connected to the network** link.

   The Access Control page displays.

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

   In the following steps, we refer to the list of blocked devices not currently connected to the network as *the list of blocked devices*.
6. To add a device to the list of blocked devices, do the following:

   a. Click the **Add** button.

      The Add Blocked Device page displays.

   b. Enter the MAC address and device name for the device that you want to block.

   c. On the Add Blocked Device page, click the **Apply** button.

      The device is added to the list of blocked devices.
7. To remove a device from the list of blocked devices, do the following:

   a. Select the check box for the device.

   b. Click the **Remove from the list** button.

The device is removed from the list of blocked devices.

8. To change the device status by allowing access for a device on the list of blocked devices, do the following:
   a. Select the check box for the device.
   b. Click the **Edit** button.

      The Edit Device Name page displays.
   c. From the **Access Control** menu, selected **Allow**.
   d. On the Edit Device Name page, click the **Apply** button.

      The device is moved to the list of allowed devices not currently connected to the network.
9. To change the device name for a device on the list of blocked devices, do the following:
   a. Select the check box for the device.
   b. Click the **Edit** button.

      The Edit Device Name page displays.
   c. In the **Device Name** field, enter a name.
   d. On the Edit Device Name page, click the **Apply** button.

      The device name is changed on the list of blocked devices.
10. Click the **Apply** button.

    Your settings are saved.

Block Internet sites and services

You can prevent access to specific Internet sites by defining keywords and domains (websites) that must be blocked. You can also block Internet services on your network from accessing the Internet.

Use keywords to block Internet sites

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

NOTE: Keyword blocking only works for website URLs that begin with http:// only. It does not work for URLs that begin with https://.

To block Internet sites:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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. Select when to block keywords:
   - **Per Schedule**: Turn on keyword blocking according to a schedule that you set. For more information, see Schedule when to block Internet sites and services on page 64.
   - **Always**: Turn on keyword blocking all the time, independent of the Schedule page.
6. In the **Type keyword or domain name here** field, enter a keyword or domain that you want to block.

   For example:
   - Specify *xxx* to block http://www.badstuff.com/*xxx*.html and any site that includes *xxx*, such as http://www.bad*xxx*stuff.com and http://www.badstuff*xxx*.org.
   - Specify the domain suffix (for example, .com) if you want to block only sites with a domain suffix such as .com. In such a situation, sites with domain suffixes such as .edu and .gov are still allowed.
   - Enter a period (**.**) to block all Internet browsing access.
7. Click the **Add Keyword** button.

   The keyword is added to the keyword list. The keyword list supports up to 32 entries.
8. Click the **Apply** button.

   Your settings are saved. Keyword blocking takes effect.

Delete keywords from the blocked list

To delete keywords from the list:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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. Do one of the following:

   - To delete a single word, select it and click the **Delete Keyword** button.

     The keyword is removed from the list.
   - To delete all keywords on the list, click the **Clear List** button.

     All keywords are removed from the list.
6. Click the **Apply** button.

   Your settings are saved.

Prevent blocking on a trusted computer

You can exempt one trusted computer from blocking. The computer that you exempt must be assigned a fixed IP address. You can use the reserved IP address feature to specify the IP address. See Manage reserved LAN IP addresses on page 91.

To specify a trusted computer:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 computer.
7. Click the **Apply** button.

   Your settings are saved.

Block services from the Internet

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

NOTE: Service blocking works only for services and applications that are using Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) for communication.

To block services:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

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

   The Block Services page displays.

5. Select when to block the services:

   - **Per Schedule**: Turn on service blocking according to a schedule that you set. For more information, see Schedule when to block Internet sites and services on page 64.
   - **Always**: Turn on service blocking all the time, independent of the Schedule page.

6. Click the **Add** button.

   The Block Services Setup page displays.

7. To add a service that is in the **Service Type** menu, select the application or service.

   The settings for this service automatically display in the fields.
8. To add a service or application that is not in the menu, select **User Defined**, and do the following:

   a. If you know that the application uses either TCP or UDP, select the appropriate protocol. Otherwise, select **TCP/UDP** (both).

   b. Enter the starting port and ending port numbers.

      If the service uses a single port number, enter that number in both fields. To find out which port numbers the service or application uses, you can contact the publisher of the application, ask user groups or newsgroups, or search on the Internet.
9. Select a filtering option:

   - **Only This IP Address**: Block services for a single computer.
   - **IP Address Range**: Block services for a range of computers with consecutive IP addresses on your network.
   - **All IP Addresses**: Block services for all computers on your network.
10. Click the **Add** button.

    Your settings are saved.

Schedule when to block Internet sites and services

When you schedule blocking, you can use the same schedule to block sites, block services, or block both. The schedule does not become active until you assign it to site blocking, service blocking, or both.

To set up a schedule for blocking:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

The Schedule page displays.

5. Specify when the schedule is active:
   - **Days to Block**: Select the check box for each day that you want to enable blocking, or select the **Every Day** check box, which automatically selects the check boxes for all days.
   - **Time of Day to Block**: Set a start and end time in 24-hour format, or select the **All Day** check box for 24-hour blocking.
6. Click the **Apply** button.

   Your settings are saved.

Set up security event email notifications

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

To set up email notifications:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Security > E-mail**.

   The E-mail page displays.
5. Select the **Turn E-mail Notification On** check box.
6. In the **Primary E-mail Address** field, type the email address to which logs and alerts must be sent.

   This email address is also used for the From address. If this field is blank, log and alert messages are not sent.
7. (Optional) In the **Secondary E-mail Address** field, type a second email address to which logs and alerts must be sent.
8. In the **Sender** field, type the name that you want to show in the email as the sender.

9. In the **Your Outgoing Mail Server** field, type the name of your ISP outgoing (SMTP) mail server (such as mail.myISP.com).

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

    If you do not know the port number, leave the default port number.
11. If your outgoing email server requires authentication, select the **My mail server requires authentication** check box, and do the following:

    a. In the **User Name** field, type the user name for the outgoing email server.

    b. In the **Password** field, type the password for the outgoing email server.
12. To send alerts when someone attempts to visit a blocked site, select the **Send Alerts Immediately** check box.

    Email alerts are sent immediately when someone attempts to visit a blocked site.
13. To send logs based on a schedule, specify these settings:

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

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

       If you select **When log is full**, **Hourly**, or **Daily**, the day setting does not apply.

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

       If you select **When log is full** or **Hourly** the time settings do not apply.
14. Click the **Apply** button.

    Your settings are saved.

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

6

Manage WiFi Settings

You can customize the router's WiFi settings.

The chapter includes the following sections:

- Change your country or region
- Disable or reenable Smart Connect
- Hide or broadcast the SSID for a WiFi network
- Enable or disable 20/40 MHz coexistence for the 2.4 GHz radio
- Change the name for a WiFi network
- Change the WiFi password or the WiFi security
- Change the 2.4 GHz, 5 GHz, or 6 GHz WiFi channel
- Change the WiFi mode
- Set up a guest WiFi network
- Manage advanced WiFi settings
- Use the WPS Wizard for WiFi connections

Change your country or region

In some countries, the router is sold with a preconfigured country or region setting and you might not be able to change it.

To view or change your country or region:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Wireless Setup page displays.
5. From the **Region** menu, select your region.

   In some locations, you cannot change this setting.
6. Click the **Apply** button.

   Your settings are saved.

Disable or reenable Smart Connect

Smart Connect is enabled by default to select the fastest WiFi band for your router. When Smart Connect is enabled, the 2.4 GHz, 5 GHz, and 6 GHz radios use the same WiFi network name (SSID) and network key (password). That means that when you connect to the router with WiFi, you see only one SSID that allows a WiFi device to connect to any of the radios.

You might want to disable Smart Connect if you prefer to manually connect your devices to a specific WiFi band (for example, to connect WiFi 6E or WiFi 7 devices to the 6 GHz band).

NOTE: If you first disable and then reenable Smart Connect and the SSID and passwords for the 2.4 GHz, 5 GHz, and 6 GHz radios do not match, the WiFi settings for the 2.4 GHz radio overwrite the WiFi settings for the 5 GHz and 6 GHz radios.

To disable or reenable Smart Connect:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Wireless Setup page displays.
5. Clear or select the **Enable Smart Connect** check box.

   By default, Smart Connect is enabled. Clearing this check box disables Smart Connect. Selecting this check box reenables Smart Connect.
6. Click the **Apply** button.

   Your settings are saved.

Hide or broadcast the SSID for a WiFi network

By default, a WiFi network broadcasts its WiFi network name (also referred to as the SSID) so that WiFi clients can detect the SSID in their scanned network lists. For additional security, you can turn off the SSID broadcast and hide the SSID so that users must know the SSID to be able to join the WiFi network.

To hide or broadcast the network name for a WiFi network:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

The Wireless Setup page displays.

5. Select or clear the **Enable SSID Broadcast** check box for the 2.4 GHz, 5 GHz, or 6 GHz radio.

   Selecting each check box enables broadcast of the SSID (the default setting) and clearing each check box hides the SSID for the corresponding band.

6. Click the **Apply** button.

   Your settings are saved.

Enable or disable 20/40 MHz coexistence for the 2.4 GHz radio

20/40 coexistence allows a 20 MHz and 40 MHz channel width to be supported simultaneously. By default, 20/40 MHz coexistence is enabled on the 2.4 GHz radio to prevent interference between WiFi networks in your environment at the expense of WiFi speed. If no other WiFi networks are present in your environment, you can disable 20/40 MHz coexistence to increase the WiFi speed on the 2.4 GHz radio to the maximum supported speed for the WiFi mode.

20/40 MHz coexistence applies to the 2.4 GHz radio.

To enable or disable 20/40 MHz coexistence for the 2.4 GHz radio:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

4. Select **Wireless**.

   The Wireless Setup page displays.

5. Select or clear the **Enable 20/40 MHz Coexistence** check box.

   Selecting this check box enables coexistence (the default setting) and clearing this check box disables coexistence.

6. Click the **Apply** button.

   Your settings are saved.

Change the name for a WiFi network

For each WiFi network, the WiFi network name (also referred to as the SSID) is randomly generated and is on the router label. You can change the default network name. The network name can be up to 32 characters long and is case-sensitive.

NOTE: If Smart Connect is enabled, the 2.4 GHz, 5 GHz, and 6 GHz radios use the same WiFi network name (SSID). To use a different SSID for each band, disable Smart Connect.

To change the name for a WiFi network:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Wireless Setup page displays.
5. In the **Name (SSID)** field, enter a new name.
6. Click the **Apply** button.

   Your settings are saved.

Change the WiFi password or the WiFi security

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

Your router comes with preset security settings, which are printed on the router label. We recommend that you use the preset security settings, but you can change the settings. We also recommend that you do not disable the WiFi security.

To change the WiFi password or the WiFi security:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Wireless Setup page displays.
5. To change the 2.4 GHz, 5 GHz, or 6 GHz WiFi password, enter a new password in the **Password (Network Key)** field.

   The password is a phrase of 8 to 63 alphanumeric characters or of exactly 64 hexadecimal characters.

   NOTE: By default, your password is hidden. To display your password, click the icon next to the **Password** field.
6. When Smart Connect is disabled, to change the WiFi security for the 2.4 GHz or 5 GHz WiFi network, select a **Security Options** radio button:
   - **None**: An open WiFi network does not provide any security. Any WiFi device can join the WiFi network.
   - **WPA2-Personal**: When Smart Connect is disabled, this is the default setting for the 2.4 GHz and 5 GHz WiFi networks. WPA2-Personal provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. If your WiFi network includes these older devices, select WPA-Personal + WPA2-Personal security.
   - **WPA-Personal + WPA2-Personal**: Enables WiFi devices that support either WPA or WPA2 to join the WiFi network. However, WPA is less secure than WPA2 and limits the speed of WiFi devices to 54 Mbps.
   - **WPA3-Personal**: Enables WiFi devices that support WPA3 to join the WiFi network. WPA3 is the latest security standard, uses SAE encryption, and is more secure than WPA2. If all devices on your WiFi network support WPA3, we recommend that you use this type of security.
   - **WPA2-Personal + WPA3-Personal**: When Smart Connect is enabled (which it is by default), this is the default setting for the 2.4 GHz and 5 GHz WiFi networks. This type of security enables WiFi devices that support either WPA2 or WPA3 to join the WiFi network. The security uses SAE and AES encryption. WPA2 (which uses AES) is less secure than WPA3 (which uses SAE).

NOTE: If you first disable and then reenable Smart Connect and the security settings for the 2.4 GHz, 5 GHz, and 6 GHz radios do not match, the security settings for the 2.4 GHz radio overwrite the WiFi settings for the 5 GHz and 6 GHz radios. If WPA2-Personal + WPA3-Personal is selected, the 2.4 GHz and 5 GHz radios use the mixed setting, while the 6 GHz radio uses WPA3. If WPA3-Personal is selected, all three bands use WPA3.

NOTE: Whether or not Smart Connect is enabled, the WiFi security for the 6 GHz WiFi network is set at WPA3-Personal. This security option enables WiFi devices that support WPA3 to join the 6 GHz WiFi network. WPA3 is the latest security standard, uses SAE encryption, and is required to join the 6 GHz WiFi network.

7. Click the **Apply** button.

   Your settings are saved.

Change the 2.4 GHz, 5 GHz, or 6 GHz WiFi channel

You can change the 2.4 GHz, 5 GHz , or 6 GHz WiFi channel.

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

When you use multiple access points, it is better if adjacent access points use channels as distant from each other as possible to reduce interference.

NOTE: If you change the 2.4 GHz, 5 GHz, or 6 GHz channel, the change also applies to the guest network.

To change the WiFi channel:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

4. Select **Wireless**.

   The Wireless Setup page displays.
5. To change the 2.4 GHz, 5 GHz, or 6 GHz WiFi channel, select a channel number from the **Channel** menu in the Wireless Network (2.4 GHz) section, Wireless Network (5 GHz) section, or Wireless Network (6 GHz) section.

   NOTE: For the 6 GHz radio, some 6 GHz WiFi clients might not find the router when the router uses a non-preferred scanning channel (PSC). We recommend that you use a channel labeled with PSC for the 6 GHz radio.
6. Click the **Apply** button.

   Your settings are saved.

Change the WiFi mode

By default, the router functions with the WiFi modes that support the highest WiFi speeds.

To change the WiFi mode:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Wireless Setup page displays.
5. In the Wireless Network (2.4 GHz) section, select a WiFi mode from the **Mode** menu.
   - **0.4 Gbps**: Allows WiFi devices to join the 2.4 GHz radio of the network and function at up to 400 Mbps (0.4 Gbps), depending on the WiFi standard that they support.
   - **0.7 Gbps**: Allows WiFi devices to join the 2.4 GHz radio of the network and function at up to 700 Mbps (0.7 Gbps), depending on the WiFi standard that they support. This mode is the default mode for the 2.4 GHz radio.
6. In the Wireless Network (5 GHz) section, select a WiFi mode from the **Mode** menu.

- **0.4 Gbps**: Allows WiFi devices to join the 5 GHz radio of the network and function at up to 400 Mbps (0.4 Gbps), depending on the WiFi standard that they support.
- **0.7 Gbps**: Allows WiFi devices to join the 5 GHz radio of the network and function at up to 700 Mbps (0.7 Gbps), depending on the WiFi standard that they support.
- **1.5 Gbps**. Allows WiFi devices to join the 5 GHz radio of the network and function at up to 1.5 Gbps, depending on the WiFi standard that they support.
- **2.9 Gbps**: Allows WiFi devices to join the 5 GHz radio of the network and function at up to 2.9 Gbps, depending on the WiFi standard that they support. This mode is the default mode for the 5 GHz radio.

7. In the Wireless Network (6 GHz) section, select a WiFi mode from the **Mode** menu.
   - **0.7 Gbps**: Allows WiFi devices to join the 6 GHz radio of the network and function at up to 700 Mbps (0.7 Gbps), depending on the WiFi standard that they support.
   - **1.4 Gbps**. Allows WiFi devices to join the 6 GHz radio of the network and function at up to 1.4 Gbps, depending on the WiFi standard that they support.
   - **2.9 Gbps**: Allows WiFi devices to join the 6 GHz radio of the network and function at up to 2.9 Gbps, depending on the WiFi standard that they support.
   - **5.8 Gbps**: Allows WiFi devices to join the 6 GHz radio of the network and function at up to 5.8 Gbps, depending on the WiFi standard that they support. This mode is the default mode for the 6 GHz radio.
8. Click the **Apply** button.

   Your settings are saved.

Set up a guest WiFi network

A guest WiFi 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 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 0.7 Gbps in the 2.4 GHz band, the guest WiFi network also functions in the 0.7 Gbps mode in the 2.4 GHz band. The channel also depends on the channel selection of the main WiFi network.

By default, these networks are disabled. You can enable one or both guest networks. You can also change the SSIDs for these networks.

To set up a guest WiFi network:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **Guest Network**.

   The Guest Network Settings page displays.
5. Configure the following settings to set up a 2.4 GHz, 5 GHz, or 6 GHz guest network, or a guest WiFi network that is active on two radios or all radios:
   - **Enable Guest Network**: By default, the guest WiFi network is disabled. To enable the guest WiFi network for the 2.4 GHz or 5 GHz WiFi band, select the **Enable Guest Network** check box.
   - **Enable SSID Broadcast**: By default, the router broadcasts the SSID of the 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, 5 GHz, or 6 GHz guest WiFi network, clear the **Enable SSID Broadcast** check box.
   - **Allow guests to see each other and access my local network**: By default, WiFi clients that are connected to the 2.4 GHz, 5 GHz, or 6 GHz 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.
   - **Guest Wireless Network Name (SSID)**: The SSID is the 2.4 GHz, 5 GHz, or 6 GHz guest WiFi network name. The default name for all three networks is NETGEAR-Guest.

     To change the SSID, type a name of maximum 32 characters in the field. The SSID is case-sensitive.
6. Select a WiFi security option for the 2.4 GHz, 5 GHz, or both the 2.4 GHz and 5 GHz radios for the guest WiFi network:
   - **None**: An open WiFi network does not provide any security, and no password is required. Any WiFi device can join the guest WiFi network.
   - **WPA2-Personal**: This is the default setting for the 2.4 GHz and 5 GHz WiFi guest networks. This type of security provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. If your guest WiFi

network includes these older devices, select WPA-Personal + WPA2-Personal security.

- **WPA-Personal + WPA2-Personal**: Enables WiFi devices that support either WPA or WPA2 to join the guest WiFi network. However, WPA is less secure than WPA2 and limits the speed of WiFi devices to 54 Mbps.
- **WPA3-Personal**: Enables WiFi devices that support WPA3 to join the guest WiFi network. WPA3 is the latest security standard, uses SAE encryption, and is more secure than WPA2. If all devices on your guest WiFi network support WPA3, we recommend that you use this type of security.
- **WPA2-Personal + WPA3-Personal**: Enables WiFi devices that support either WPA2 or WPA3 to join the guest WiFi network. This type of security uses SAE and AES encryption. WPA2 (which uses AES) is less secure than WPA3 (which uses SAE).

NOTE: The WiFi security for the 6 GHz WiFi network is set at WPA3-Personal. This security option enables WiFi devices that support WPA3 to join the 6 GHz WiFi network. WPA3 is the latest security standard, uses SAE encryption, and is required to join the 6 GHz WiFi network.

7. Set a password for the selected WiFi Security option by typing a passphrase in the **Password (Network Key)** field.

   The password is a phrase of 8 to 63 alphanumeric characters or of exactly 64 hexadecimal characters.

   NOTE: By default, your password is hidden. To display your password, click the icon next to the **Password** field.

8. Click the **Apply** button.

   Your settings are saved.

Manage advanced WiFi settings

CAUTION: Take extra care changing advanced WiFi settings because incorrect configuration might affect the WiFi function of the router.

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 multiple schedules, and you can set up separate schedules for the 2.4 GH and 5 GHz radios.

To set up a WiFi schedule for a radio:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Wireless Settings page displays.
5. Click the **Add a new period** button for a radio.

   The Turn off wireless signal by schedule 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.
7. Click the **Apply** button.

   The Wireless Settings page displays.

   The new schedule displays in the table. (You can edit or delete the schedule.)
8. Select the **Turn off wireless signal by schedule** check box for the radio to activate the schedule.

   Selecting this check box enables all WiFi schedules for the radio radio and clearing this check box disables all WiFi schedules for the radio. By default, no WiFi schedule is set up and the check box is disabled.
9. Click the **Apply** button.

   Your settings are saved.

Enable or disable MU-MIMO

Multiuser multiple input, multiple output (MU-MIMO) improves performance when many WiFi clients that are MU-MIMO-capable transfer data at the same time. For MU-MIMO to function, WiFi clients must support MU-MIMO (some older devices do not), and they must be connected to the 5 GHz WiFi band. This feature is enabled by default, but you can disable it.

To enable or disable MU-MIMO:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Wireless Settings page displays.
5. Scroll down and select or clear the **Enable MU-MIMO** check box.

   Selecting this check box enables MU-MIMO (the default setting). Clearing this check box disables MU-MIMO.
6. Click the **Apply** button.

   Your settings are saved.

Change the fragmentation length, CTS/RTS threshold, or preamble mode for a radio

For most WiFi networks, the default fragmentation length, CTS/RTS threshold and preamble mode work fine and we recommend that you do not change the settings. (In general, these settings are intended for WiFi testing.)

CAUTION: We recommend that you 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 a radio unexpectedly.

NOTE: If the Smart Connect feature is enabled, the fragmentation length, CTS/RTS threshold, and preamble mode for the 2.4 GHz radio, 5 GHz radio, and 6 GHz radio are combined. That means that you cannot change these settings for the 2.4 GHz radio, 5 GHz radio, or 6 GHz radio individually.

To change the fragmentation length, CTS/RTS threshold, or preamble mode for a radio:

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

A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

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

   The Advanced Wireless Settings page displays.

5. In the **Fragmentation Length (256-2346)** field for a radio, enter a value from 256 to 2436.

   The default value is 2346.

6. In the **CTS/RTS threshold (1-2347)** field for a radio, enter a value from 1 to 2437.

   The default value is 2347.

7. From the **Preamble Mode** menu for a radio, select the preamble mode:

   - **Long Preamble**: A long transmit preamble might provide a more reliable connection or a slightly longer range.
   - **Short Preamble**: A short transmit preamble might give better performance.

   CAUTION: Incorrect settings might disable the radio's WiFi broadcast unexpectedly.

8. Click the **Apply** button.

   Your settings are saved.

Use the WPS Wizard for WiFi connections

WPS (Wi-Fi Protected Setup) lets you connect a WPS-enabled device to your WiFi network without typing the WiFi password. Instead, you push a software button in the router web interface or enter a PIN to connect.

If you use the push button method, the 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 device that you are trying to connect.

NOTE: You cannot use the WPS Wizard to connect a device to a guest network.

Use the WPS Wizard with the push button

To use the push button method to connect a WiFi device to your WiFi network, the device must have either a physical button or a software button.

To use the WPS Wizard with the push button:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > WPS Wizard**.

   A note explaining WPS displays.
5. Click the **Next** button.

   The Add WPS Client page displays.

   By default, the **Push Button (recommended)** radio button is selected.
6. Click the green **WPS** software button on the page.
7. Within two minutes, go to the WPS-enabled device and use its WPS software to connect to the WiFi network.

   The WPS process automatically sets up the WPS-enabled device with the network password when it connects. The router web interface displays a confirmation message.

Use the WPS Wizard with a PIN

To use a PIN to connect a WiFi device to your WiFi network, you must know the PIN of the device.

To use the WPS Wizard with a PIN:

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

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

The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > WPS Wizard**.

   A note explaining WPS displays.

5. Click the **Next** button.

   The Add WPS Client page displays.

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

6. Select the **PIN Number** radio button.
7. In the **Enter Clients' PIN** field, enter the PIN of the device.
8. Click the **Next** button.

   For four minutes, the router attempts to find the WiFi device.

9. Within four minutes, go to the WiFi device and use its WPS software to join the network without entering a password.

   The WPS process automatically sets up the WPS-enabled device with the network password when it connects. The router web interface displays a confirmation message.

7

Manage the WAN and LAN Network Settings

You can customize the router's wide area network (WAN) settings for the Internet port and local area network (LAN) settings for local devices. We recommend that you install the router and connect it to the Internet before you change its network settings.

This chapter contains the following sections:

- Manage the WAN settings
- Change the LAN IP address settings or RIP settings
- Set the IP addresses that the router assigns
- Disable the DHCP server feature in the router
- Manage reserved LAN IP addresses
- Manage custom static routes
- Set up an IPTV port or a bridge for a port group or VLAN tag group
- Manage Ethernet LAN port aggregation to a LAN device

Manage the WAN settings

You can change security and other settings that determine how the router interacts with the Internet, also known as the wide area network (WAN).

Change the WAN security settings

The wide area network (WAN) security settings include port scan protection and denial of service (DoS) protection, which can protect your local area network (LAN) against many common cyber attacks. By default, DoS protection is enabled and a port scan is rejected.

You can also enable the router to respond to a ping to its Internet port. This feature allows your router to be discovered from the Internet. We recommend that you enable this feature only as a diagnostic tool or if a specific reason exists.

To change the default WAN security settings:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 protection for port scans and DoS attacks, select the **Disable Port Scan and DoS Protection** check box.
6. To enable the router to respond to a ping request from the Internet, select the **Respond to Ping on Internet Port** check box.
7. Click the **Apply** button.

   Your settings are saved.

Set up a default DMZ server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work correctly with them, but other applications might not function well. In some cases, one local computer can run the application correctly if the IP address for that computer is entered as the default DMZ server.

WARNING: DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

The router usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or is not accessing a service that you configured on the Port Forwarding/Port Triggering page. Instead of discarding this traffic, you can specify that the router forwards the traffic to one computer on your network. This computer is called the default DMZ server.

To set up a default DMZ server:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The WAN Setup page displays.
5. Select the **Default DMZ Server** check box.
6. Type the IP address.

   This must be a static IP address. For more information, see Manage reserved LAN IP addresses on page 91.
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 (such as video streaming) it is interested in from the Internet. If you do not need this feature, leave it disabled, which is the default setting.

To enable IGMP proxying:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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.

   Clearing the **Disable IGMP Proxying** check box enables IGMP proxying and selecting the **Disable IGMP Proxying** check box disables IGMP proxying. By default, IGMP proxying is disabled.
6. Click the **Apply** button.

   Your settings are saved.

Manage NAT filtering

Network Address Translation (NAT) filtering determines how the router processes inbound traffic. Secured NAT filtering blocks more unsolicited traffic from the Internet but might prevent some online games, point-to-point applications, or multimedia applications from working. Open NAT filtering provides a less secured firewall but allows almost all Internet applications to work. Secured NAT filtering is the default setting.

To change the default NAT filtering settings:

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

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

The user name is **admin**. The password is the one that you specified when you set up your router. 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**: Blocks more unsolicited traffic from the Internet but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. This is the default setting.
   - **Open**: Provides a 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 voice over IP (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 disable the SIP ALG:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 **Disable SIP ALG** check box.

   Selecting the **Disable SIP ALG** check box disables the SIP ALG and clearing the **Disable SIP ALG** check box enables the SIP ALG. By default, the SIP ALG is enabled.

6. Click the **Apply** button.

Your settings are saved.

Change the LAN IP address settings or RIP settings

The router is preconfigured to use private IP addresses on the local area network (LAN) side and to act as a Dynamic Host Configuration Protocol (DHCP) server. We also refer to the LAN IP address settings as the LAN TCP/IP settings.
The router's default LAN IP configuration is as follows:

- **LAN IP address**: 192.168.1.1
- **Subnet mask**: 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings.

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

Router Information Protocol (RIP) allows a router to exchange routing information with other routers on the same network.

To change the LAN IP address settings or RIP settings:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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. To change the LAN IP address settings, do the following:
   a. In the **IP Address** field, type the IP address.
   b. In the **IP Subnet Mask** field, type the subnet mask of the router.

The IP address and subnet mask specify the IP address range that the devices on your network can use.

6. To change the RIP settings, do the following:

   a. Select the RIP direction:

      - **Both**: The router broadcasts its routing table periodically and incorporates information that it receives.
      - **Out Only**: The router only broadcasts its routing table periodically.
      - **In Only**: The router only incorporates the RIP information that it receives.

   b. Select the RIP version:

      - **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.

   If you changed the LAN IP address of the router, you are disconnected when this change takes effect.

8. To reconnect, close your browser, relaunch it, and log in to the router.

Set the IP addresses that the router assigns

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 connected to the LAN. The assigned default gateway address is the LAN address of the router.

These addresses must be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, define a range between 192.168.1.2 and 192.168.1.254, although you can save part of the range for devices with fixed addresses.

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

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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.
6. Specify the range of IP addresses that the router assigns:

   a. In the **Starting IP Address** field, type the lowest number in the range.

   b. In the **Ending IP Address** field, type the number at the end of the range of IP addresses.
7. Click the **Apply** button.

   Your settings are saved.

The router delivers the following address information to any LAN device that requests a DHCP address:

- An IP address from the range that you define
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- DNS server IP address (the router's LAN IP address)

Disable the DHCP server feature in the router

By default, the router acts 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 manually specify the network settings of all your devices.

To disable the DHCP server feature in the router:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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.
7. (Optional) If this service is disabled and no other DHCP server is on your network, set your device IP addresses manually so that the devices can access the router and the Internet.

Manage reserved LAN IP addresses

When you specify a reserved IP address for a device on the LAN, that device always receives the same IP address each time it requests an IP address from the router's DHCP server (for example, when the device restarts). Assign reserved IP addresses to devices or servers that require permanent IP settings.

Reserve an IP address

To reserve an IP address:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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. To reserve the IP address for a device that the router detects automatically, in the Address Reservation Table, select the radio button for the device.
7. To manually reserve an IP address for a device, do the following:
   a. In the **IP Address** field, type the IP address to assign to the device.

      Choose an IP address from the router's LAN subnet, such as 192.168.1.x. (In a typical LAN subnet, IP addresses 192.168.1.0, 192.168.1.1, and 192.168.1.255 are reserved and cannot be used. 192.168.1.0 and 192.168.1.255 are not used by any devices.)

   b. In the **MAC Address** field, type the MAC address of the device.
   c. In the **Device Name** field, type a name for the device.
8. Click the **Add** button.

   Your settings are saved. The reserved address is entered into the Address Reservation table on the LAN Setup page.

The reserved address is not assigned until the next time the device requests an IP address from the router's DHCP server. Restart the device to force the device to request an IP address from the router.

Edit a reserved IP address

To edit a reserved address entry:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

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

   The LAN Setup page displays.

5. Select the radio button next to the reserved address that you want to edit.
6. Click the **Edit** button.

   The Address Reservation page displays.
7. Change the settings.
8. Click the **Apply** button.

   Your settings are saved.

Delete a reserved IP address entry

To delete a reserved address entry:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The LAN Setup page displays.
5. Select the radio button next to the reserved address that you want to delete.
6. Click the **Delete** button.

   The address is removed.

Manage custom static routes

For almost all Internet traffic, routes are automatically and dynamically selected. You can also set up a fixed, static route. Typically, you only need to add static routes when you have more than one router or multiple IP subnets on your network.

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

- Your main Internet access is through a cable modem to your ISP. The cable modem is connected to your router.
- Your network also includes an ADSL router that you use to access a remote office site. This ADSL router is connected to a DSL modem, which is used on-demand only.

- Your LAN subnet is 192.168.1.0, and the ADSL router's address on your LAN is 192.168.1.100.
- The public IP address range at the remote office site is 134.177.0.0.

When you set up your router, two implicit static routes were created:

1. A default route was created between your router and your ISP's gateway.
2. A second static route was created between your router and your LAN for all 192.168.1.0 addresses.

With this configuration, if you try to access a device on the 134.177.0.0 network at the remote office site, your router forwards your request to your ISP. In turn, the ISP forwards your request to the remote office site, where the firewall will deny the request.

In this situation, you must define a static route, telling your router to access 134.177.x.x addresses through your ADSL router at its LAN address of 192.168.1.100.

Here is an example static route setting for this configuration:

- **Destination IP address and subnet mask settings**: The route applies to all addresses at the remote site, so set the destination IP address to 134.177.0.0 and the subnet mask to 255.255.0.0.
- **Gateway IP address**: Traffic for addresses in the 134.177.x.x network must be forwarded to the ADSL router, so set the gateway IP address to 192.168.1.100 (the ADSL router's address on your LAN).
- **Private route**: Make the static route private as a security precaution in case Routing Information Protocol (RIP) is activated. A private route is not reported in RIP messages.
- **Active**: Select the Active check box to ensure the route is active.
- **Metric**: Set a low value for the metric (for example, 2).

Set up a static route

To set up a static route:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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.

   Static route configuration options display.

6. In the **Route Name** field, type a name for this static route (for identification purposes only).
7. To limit access to the LAN only, select the **Private** check box.

   If the **Private** check box is selected, the static route is not reported in RIP.

8. To prevent the route from becoming active, 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.

9. Enter the following settings:
   - **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 for routing the traffic to the final destination or host.

     The IP address of the gateway must be on the same LAN segment as the router.
   - **Metric**: Enter a number from 2 through 15.

     This value represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.

10. Click the **Apply** button.

    Your settings are saved. The static route is added to the table on the Static Routes page.

Edit a static route

To edit a static route:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 table, select the radio button for the route.
6. Click the **Edit** button.

   Static route configuration options display.

7. Edit the route information.
8. Click the **Apply** button.

   Your settings are saved.

Delete a static route

To delete a static route:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 table, select the radio button for the route.
6. Click the **Delete** button.

   The route is removed from the table.

Set up an IPTV port or a bridge for a port group or VLAN tag group

If you subscribe to an Internet Protocol television (IPTV) service (a TV streaming service) and your IPTV service requires an intranet address, you can set up an IPTV port.

Some devices, such as an IPTV, cannot function behind the router's network address translation (NAT) service or firewall. For example, an IPTV port might require an IP address within the Internet service provider's (ISP's) network (also called an ISP intranet address).

The way you set up an IPTV port is by creating a bridge connection from the router's Internet port to the LAN port to which the IPTV device is connected. When IPTV is connected through WiFi, the router must also support a bridge connection from the Internet port to the WiFi network. The designated LAN port or WiFi network effectively becomes an IPTV port with direct access to the WAN without going through NAT.

Based on what your ISP requires for the device to connect to the ISP's network directly, you can enable the bridge between the IPTV device and the router's Internet port with or without a VLAN tag.

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

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 the IPTV device and the router's Internet interface without a virtual local area network (VLAN) tag.

A bridge with a port group does not use VLAN tags and prevents packets that are sent between the IPTV device and the router's Internet port from being processed through the router's network address translation (NAT) service.

To configure a port group and enable the bridge:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 / Bridge group** check box.

   The page expands.
6. Select the **By bridge group** radio button.

7. Select a Wired Ports check box or a Wireless check box:
   - **Wired Ports**: If your device is connected to an Ethernet LAN port on the router, select the Wired Ports check box that corresponds to the Ethernet LAN port on the router to which the device is connected.
   - **Wireless**: If your device is connected to your router's WiFi network, select the Wireless check box that corresponds to the router's WiFi network to which the device is connected.

   NOTE: You must select at least one Wired Ports or Wireless check box. You can select more than one check box. Depending on your configuration, other devices connected to the specified ports or WiFi networks might not be able to access the public Internet.
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 the IPTV device and the router's Internet interface with a virtual local area network (VLAN) tag.

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

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

To add a VLAN tag group and enable the bridge:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 / Bridge group** check box.

   The page expands.
6. Select the **Enable VLAN Tag** radio button.

   The page expands.

   The table includes a default VLAN enabled for normal Internet access. The VLAN's ID is 10 and has all Ethernet LAN ports and WiFi networks as members.
7. Click the **Add** button.

   The Add VLAN Rule page displays.
8. Specify the following settings for the VLAN tag group:
   - **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 (lowest priority) to 7 (highest priority).
9. Select the check box for a wired Ethernet LAN port or wireless network.

   If your device is connected to an Ethernet LAN port on the router, select the wired Ethernet LAN port check box that corresponds to the Ethernet LAN port on the router to which the device is connected. If your device is connected to your router's WiFi network, select the WiFi check box that corresponds to the router's WiFi network to which the device is connected.

   You must select at least one Ethernet LAN port or WiFi network. You can select more than one port or WiFi network. Depending on your configuration, other devices connected to the specified ports or WiFi networks might not be able to access the public Internet.
10. Click the **Add** button.

    Your settings are saved.

    The VLAN tag group is added and automatically enabled. The VLAN / Bridge Settings page displays again.

Manage Ethernet LAN port aggregation to a LAN device

Ethernet LAN aggregation lets you aggregate two Ethernet LAN ports on your router to improve the aggregated file transfer speed. Ethernet LAN port aggregation is also referred to as link aggregation, teaming port, and port trunking.

To set up Ethernet LAN port aggregation to a LAN device that is configured for 802.3ad Link Aggregation Control Protocol (LACP), first configure Ethernet LAN port aggregation for the LAN port 1 and LAN port 2 on your router, and then connect these ports to the two aggregated ports on the LAN device. If you do not configure port aggregation in this order, a network loop occurs, and your network might be shut down.

We refer to Ethernet LAN port aggregation for LAN devices as LAN port aggregation.

WARNING: Do not connect an *unmanaged* switch to LAN port 1 and LAN port 2 on your router if these ports are aggregated. Otherwise, a network loop occurs, and your network might be shut down.

Set up LAN port aggregation to a LAN device

If you are connecting a LAN device such as a switch or NAS, make sure that your LAN device supports either 802.3ad LACP or static LAGs.

To set up LAN port aggregation to a LAN device:

1. Set up LAN port aggregation on your LAN device before connecting it to your router.

   NOTE: You must also enable link aggregation on your router before you connect your device to LAN ports 1 and 2 on the router, otherwise you will create a network loop.

   For information about how to set up LAN port aggregation on your LAN device, see the documentation that came with your LAN device.

   The following steps describe how to log in to your router and enable LAN port aggregation on the router.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Ethernet Settings**.

   The Ethernet Settings page displays.
6. In the LAN Port Aggregation section, select a LAN port aggregation mode (by default, LAN port aggregation is disabled):

- **Enable (LACP-IEEE 802.3ad**): After you connect the Ethernet cables (see the following step), the router communicates with the LAN device that is connected to LAN ports 1 and 2 on your router, and checks to see if LAN port aggregation is supported on the LAN device. If LAN port aggregation is supported, the router automatically trunks LAN ports 1 and 2. If not, LAN ports 1 and 2 work as independent LAN ports. We recommend that you select this mode unless your LAN device can support a static LAG only.
- **Static**: If your device supports a static LAG only, select this mode. Otherwise, we recommend that you select the **Enable (LACP-IEEE 802.3ad)** radio button instead.

7. Click the **Apply** button.

   Your settings are saved.

   After you complete the next step, the Ethernet Port Aggregation Status field displays if Ethernet port aggregation is active or inactive.
8. Physically connect your LAN device to LAN ports 1 and 2 on the router.

View or change the router LAN port aggregation mode

To view or change your router's LAN port aggregation mode:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Ethernet Settings page displays.

   In the LAN Port Aggregation section, the Ethernet Port Aggregation Status field shows whether port aggregation is active:

   - **Inactive**: No link aggregation LAN device is connected to Ethernet LAN ports 1 and 2 on your router.
   - **Active**: A link aggregation LAN device is connected to Ethernet LAN ports 1 and 2 on your router.

5. To change the LAN port aggregation mode, select one of the following radio buttons:
   - **Disable**: This mode is selected by default. This mode disables LAN port aggregation on your router. LAN ports 1 and 2 can be used as independent Ethernet LAN ports.
   - **Enable (LACP-IEEE 803.3ad**): After you connect the Ethernet cables, the router communicates with the LAN device that is connected to LAN ports 1 and 2 on your router, and checks to see if LAN port aggregation is supported on the LAN device. If LAN port aggregation is supported, the router automatically trunks LAN ports 1 and 2. If not, LAN ports 1 and 2 work as independent LAN ports. We recommend that you select this mode unless your LAN device can support a static link aggregation group (LAG) only.
   - **Static**: If your device supports a static LAG only, select this mode. Otherwise, we recommend that you select the **Enable (LACP-IEEE 802.3ad)** radio button instead.

     NOTE: You must also enable link aggregation on your router before you connect your device to LAN ports 1 and 2 on the router, otherwise you will create a network loop.
6. If you made changes, click the **Apply** button.

   Your settings are saved.

8

Optimize Performance

You can set up the router to optimize performance.

This chapter contains the following sections:

- Enable QoS
- Set the Internet bandwidth for your router
- Update the QoS database
- Manage Wi-Fi Multimedia QoS
- Improve network connections with Universal Plug and Play

Enable QoS

Quality of Service (QoS) helps improve your router's Internet traffic management capabilities through better application and device identification, bandwidth allocation, and traffic prioritization techniques. QoS resolves traffic congestion when the Internet bandwidth is limited and different demands compete for bandwidth.

QoS does not increase your total Internet bandwidth or WiFi throughput.

To enable QoS:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The QoS page displays
5. Select the **Enable QoS** check box.
6. Click the **Apply** button.

   Your settings are saved.

Set the Internet bandwidth for your router

You can let a speed test automatically set the Internet bandwidth for your router, or you can do so manually.

NOTE: A speed test does not increase your total Internet bandwidth or WiFi throughput.

To set the Internet bandwidth for your router:

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

A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

4. Select **QoS**.

   The QoS page displays.

5. Select the **Enable Speed Test** check box.
6. Select how the Internet bandwidth is set for the router:

   - **Let Speedtest detect my Internet bandwidth**: We recommend that you use the speed test to detect your Internet bandwidth.

     To use the speed test, do the following:

     a. For more accurate speed test results, make sure that no other devices are accessing the Internet.
     b. Select the **Let Speedtest detect my Internet bandwidth** radio button.
     c. Click the **Take a Speedtest** button.

        The speed test determines your Internet bandwidth and sets it for the router.

   - **I want to define my Internet Bandwidth**: If you know what your download and upload speed are, select this radio button and enter your download and upload speeds in the fields.

7. Click the **Apply** button.

   Your settings are saved.

Update the QoS database

The router uses a QoS database of the most popular applications and services to automatically optimize your bandwidth utilization for the applications accessing the Internet on your network. You can manually update this database or let the router automatically update it.

To enable or disable the automatic Dynamic QoS database update:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The QoS page displays
5. To let the router automatically update the QoS database, select the **Automatically update performance optimization database** check box.

   When you enable QOS, this check box is automatically selected.
6. To update the QoS database immediately, click the **Update Now** button.

   The router connects to a Netgear server.
7. Click the **Apply** button.

   Your settings are saved.

Manage Wi-Fi Multimedia QoS

Wi-Fi multimedia (WMM) Quality of Service (QoS) prioritizes WiFi voice and video traffic over the WiFi connection. WMM QoS is automatically enabled for the router.

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

NOTE: We recommend that you do not disable the WMM settings. If you disable the WMM settings for a radio, the maximum WiFi speed might be lowered.

To disable the WMM settings:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Setup > QoS Setup**.

   The QoS page displays.
5. Click the **WMM** tab.

   The WMM check boxes display.
6. Clear the **Enable WMM (Wi-Fi multimedia) settings** check box for one or more radios.
7. Click the **Apply** button.

   Your settings are saved.

Improve network connections with Universal Plug and Play

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

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

To enable or disable Universal Plug and Play:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The UPnP page displays.
5. Select the **Turn UPnP On** check box.

   By default, this check box is selected. UPnP for automatic device configuration can be enabled or disabled. If you clear the **Turn UPnP On** check box, the router does not allow any device to automatically control router resources, such as port forwarding.

6. In the **Advertisement Period** field, type the advertisement period in minutes.

   The advertisement period specifies how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points receive current device status at the expense of more network traffic. Longer durations can compromise the freshness of the device status but can significantly reduce network traffic.

7. In the **Advertisement Time to Live** field, type the advertisement time to live in hops.

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

9

Manage and Monitor Your Router

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

This chapter contains the following sections:

- Update the router firmware
- Change the admin password
- Enable admin password reset
- Reset the admin password
- Use HTTPS to access the router
- Change the router's device name
- Manage the router configuration file
- Monitor the router and network
- Monitor, meter, and control Internet traffic
- Set the NTP server
- Set your time zone and daylight saving time
- Set up the router as a WiFi access point
- Return the router to router mode
- Manage LED blinking or turn off LEDs
- Connect to your router with Anywhere Access
- Return the router to its factory default settings

Update the router firmware

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

Check for new firmware and update the router

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

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

To check for new firmware and update your router:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Router Update**.

   The Router Update page displays.
5. Click the **Check** button.

   The router finds new firmware information if any is available and displays a message asking if you want to download and install it.
6. Click the **Update** button.

   The router locates and downloads the firmware and begins the update.

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

When the update is complete, your router restarts. The update process typically takes about one minute. Read the new firmware release notes to find out if you must reconfigure the router after updating.

Manually upload firmware to the router

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

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

To manually upload a firmware file to your router:

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

   NOTE: The correct firmware file uses an `.img` or `.chk` extension.

2. If available, read the firmware release notes to find out if you must reconfigure the router after uploading.
3. Launch a web browser from a computer or mobile device that is connected to the router network.
4. Enter **http://www.routerlogin.net**.

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
6. Select **ADVANCED > Administration > Router Update**.

   The Router Update page displays.
7. Select the **Manual Update** tab.

   The Manual Update page displays.
8. Click the **Browse** button.
9. Find and select the firmware file on your computer.
10. Click the **Upload** button.

    The router begins the upload.

    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.

When the upload is complete, your router restarts. The upload process typically takes about one minute.

Manage the firmware update settings

You can set the router to automatically update to future firmware versions as they become available.

To manage automatic updates for future firmware versions:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Router Update**.

   The Router Update page displays.
5. In the Router Auto Firmware Update section, select one of the following radio buttons.
   - **Enable**: The router automatically updates to future firmware versions as they become available. This is the default setting. We recommend that you keep this setting so that you get the latest security and feature updates as soon as they are available.
   - **Disable**: The router does not automatically update to future firmware versions. You must manually update to future firmware versions.
6. Click the **Apply** button.

   Your settings are saved.

Change the admin password

The admin password is also called the router login password. It is the password that you need to log in to the router with the admin user name when you use a web browser to access the router.

The first time that you logged in to the router, you set the admin password. You can change this password.

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

To change the password for the admin user name:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Set Password**.

   The Set Password page displays.
5. Type the old password in the **Old Password** field.
6. Type the new password in the **Set Password** and **Repeat New Password** fields.
7. Click the **Apply** button.

   Your settings are saved.

Enable admin password reset

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

To enable password reset:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 Reset** check box.
6. Select two security questions and provide answers to them.
7. Click the **Apply** button.

   Your settings are saved.

Reset the admin password

If you set up the password reset feature (see Enable admin password reset on page 113), you can reset your router admin password if you forgot it. This reset process is supported in Chrome, Safari, Firefox, Edge, and Internet Explorer.

To reset your router admin password:

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

   A login window displays.
3. Click the **Cancel** button.

   If password reset is enabled, you are prompted to enter the serial number of the router.

   The serial number is on the router label.
4. Enter the serial number of the router.
5. Click the **Continue** button.

   The Router Password Reset page displays.
6. Enter the answers to your security questions.
7. Click the **Continue** button.

   New password fields display.
8. Type a new admin password, confirm your new password, and set new security questions and answers.
9. Click the **Next** button.

   The page displays a confirmation.
10. Click the **Login** button.

    A login window opens.
11. With your new password, log in to the router.

Use HTTPS to access the router

You can configure the router to always require secure HTTP (HTTPS) connections between your web browser and the router web interface, for example, "https://www.routerlogin.net". When you enable the HTTPS requirement, connection requests to the router web interface that specify HTTP are automatically converted to HTTPS.

NOTE: After you enable the HTTPS requirement, when you enter **http://www.routerlogin.net**, your browser might display a security warning because of the self-signed certificate on the router. This is expected behavior. You can proceed, or add an exception for the security warning. For more information, visit kb.netgear.com/000062980/what-to-do-incase-of-security-message.

To require HTTPS connections:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Web Services Management**.

   The Web Services Management page displays.
5. Select the **Always Use HTTPS to Access Router** check box.
6. Click the **Apply** button.

   Your settings are saved.

Change the router's device name

The router's default device name is based on its model number. This device name displays in the file manager when you browse your network.

To change the router's device name:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Setup > Device Name**.

   The Device Name page displays.
5. In the **Device Name** field, type a new name.

   Type up to 32 alphanumerical characters.
6. Click the **Apply** button.

   Your settings are saved.

Manage the router configuration file

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

Back up the settings

To back up the router's configuration settings:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

The BASIC Home page displays.

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

   The Backup Settings page displays.

5. Click the **Back Up** button.
6. Follow the direction of your browser to save the `.cfg` file.

   A copy of the current settings is saved in the location that you specify.

   NOTE: Because .cfg files downloaded from the public Internet can contain malicious data, some web browsers might display a warning message that asks if you want to keep the backup settings .cfg file from your router. The .cfg file that your router generates is safe. You can clear any warning messages that your browser might display before downloading.

Restore the settings

To restore configuration settings that you backed up:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

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

   The Backup Settings page displays.

5. Click the **Browse** button to find and select the `.cfg` file.
6. Click the **Restore** button.

   The file is uploaded to the router and the router restarts.

   WARNING: Do not interrupt the restoration process.

Erase the settings

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

To erase the settings:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Backup Settings**.

   The Backup Settings page displays.
5. Click the **Erase** button.

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

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

Monitor the router and network

You can view information about the router and the Internet and WiFi settings, view devices on the network, view and manage logs of router activity, and view packet statistics.

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 and WiFi settings:

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

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

The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED**.

   The ADVANCED Home page displays.

   The page displays panes for the router, Internet port, WiFi networks, and guest WiFi networks.

   The information on this page uses the following color coding:

   - **Green icon**: The Internet connection is fine and no problems exist. For a WiFi network, the network is enabled and secured.
   - **Red icon**: Configuration problems exist for the Internet connection. For a WiFi network, the network is disabled or down.
   - **Amber icon**: The Internet port is configured but cannot get an Internet connection (for example, because the cable is disconnected), a WiFi network is enabled but unprotected, or another situation requires your attention.

View devices currently on the network

You can view all devices that are currently connected to your network. If you are using VPN, you can also view the remote devices that are connected to your router through VPN.

To view devices on the network:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **Attached Devices**.

   The following information is displayed:

   - **Status**: Displays only if network access control (see Network access control list on page 54) is enabled. The field displays if a device is allowed or blocked.
   - **Connection Type**: Either wired or the WiFi band for the connection
   - **Device Name**: The device name, if known

- **IP Address**: The IP address that the router assigned to this device when it joined the network. This address can change if a device is disconnected and rejoins the network.
- **MAC Address**: The unique MAC address for each device. The MAC address is typically shown on the product label of the device.

  NOTE: Some iOS and Android devices display a private or randomized MAC address when connecting to WiFi. If a device does not connect to your WiFi network for a while, it might connect with a different MAC address next time. You can disable this setting on your iOS or Android device.

If you configured VPN (see Use OpenVPN to Access Your Network on page 156) and any VPN client devices are connected to the router, the following information is displayed in a separate table:

- **Device Name**: The device name, if known
- **Remote IP Address**: The device IP address at the remote location
- **Local IP Address**: The device IP address at the router network
- **Connection Time**: The time that the VPN connection is active

5. To edit the detected device type, model, or name that displays on the page, do the following:
   a. Select the check box for the device.
   b. Click the **Edit** button.

      The Edit Device page displays.
   c. From the **Device Type** menu, select another type than the detected type.
   d. In the **Device Model** field, type another model than the detected model.
   e. In the **Device Name** field, type another name than the detected name.
   f. Click the **Apply** button.

      You changes are saved. These changes apply only to how the device is displayed on the Attached Device page. (The device itself is not changed.)
6. To update this page, click the **Refresh** button.

View and manage logs of router activity

The logs are a detailed record of numerous router actions. When the Block Sites function is enabled, the logs also show access attempts to websites. Up to 256 entries are stored in the log.

To view and manage logs:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Logs**.

   The Logs page displays and shows information such as the following:

   - **Action**: The action that occurred, such as whether Internet access was blocked or allowed
   - **Source IP**: The IP address of the initiating device for the log entry
   - **Target address**: TWhen the Block Sites function is enabled, the name or IP address of the website or news group visited or to which access was attempted
   - **Date and time**: The date and time the log entry was recorded

   Other information might be displayed.
5. To customize the logs, scroll down and clear or select the check boxes in the Include in Log section.
6. If you make changes, click the **Apply** button.

   Your settings are saved.
7. To refresh the log screen, click the **Refresh** button.
8. To email the log immediately, click the **Send Log** button.

   You must set up email notifications in order to receive the logs. The router emails the logs to the address that you specified when you set up email notifications. For more information, see Set up security event email notifications on page 65.
9. To clear the log entries, click the **Clear Log** button.

View the Internet connection status or renew the connection

You can view the Internet connection status and, if necessary, manually restart the connection.

The information in this section applies to Internet connections that do not require you to log in to your ISP, L2TP connections, and PPTP connections.

To view the Internet connection status or renew the connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The ADVANCED Home page displays.
5. In the Internet Port pane, click the **Connection Status** button.

   The Connection Status pop-up window displays. The information that is shown depends on the type of Internet connection.

   For example, if your Internet connection does not require a login and the router receives an IP address automatically, the window displays the following information:

   - **IP Address**: The IP address that is assigned to the router
   - **Subnet Mask**: The subnet mask that is assigned to the router
   - **Default Gateway**: The IP address for the default gateway that the router communicates with
   - **DHCP Server**: The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router
   - **DNS Server**: The IP address of the Domain Name Service server that provides translation of network names to IP addresses
   - **Lease Obtained**: The length of time that the IP address lease is effective
   - **Lease Expires**: The remaining time before the IP address lease expires
6. To release (stop) the Internet connection, click the **Release** button.

   If you are using a PPTP or L2TP connection, the name of the button might be different.
7. To renew (restart) the Internet connection, click the **Renew** button.

   If you are using a PPTP or L2TP connection, the name of the button might be different.

View the PPPoE Internet connection status or renew the connection

If your router is set up to use a PPPoE Internet connection, you can view the PPPoE connection status and, if necessary, manually restart the connection.

To view the PPPoE Internet connection status or renew the connection:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 displays. The information that is shown is specific to a PPPoE connection.
6. To renew (restart) the PPPoE connection, click the **Connect** button.

   The router continues to attempt to connect. If the router does not 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.

View the packet statistics of the Internet and LAN ports and WiFi networks

To view the packet statistics of the Internet and LAN ports and WiFi networks:

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

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

The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED**.

   The ADVANCED Home page displays.

5. In the Internet Port pane, click the **Show Statistics** button.

   The Show Statistics pop-up window displays and shows the following information:

   - **System Up Time**: The time elapsed since the router was last restarted.
   - **Port**: The statistics for the WAN (Internet) port, LAN (Ethernet) ports, and WLANs (WiFi networks). For each port, the window displays the following information:
     - **Status**: The link status of the port.
     - **TxPkts**: The number of packets transmitted on this port since the router was last started.
     - **RxPkts**: The number of packets received on this port since the router was last started.
     - **Collisions**: The number of collisions on this port since the router was last started.
     - **Tx B/s**: The average (outbound) bandwidth used on the WAN and LAN ports since startup, in bytes per second.
     - **Rx B/s**: The average reception (inbound) bandwidth used on the WAN and LAN ports since startup, in bytes per second.
     - **Up Time**: The time elapsed since this port acquired the link.
   - **Poll Interval**: The interval at which the statistics are updated on this page.

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

Monitor, meter, and control Internet traffic

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

Start the traffic meter without traffic volume restrictions

You can monitor the traffic volume without setting a limit.

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

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.

   By default, no traffic limit is specified and the traffic volume is not controlled.
6. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
7. To start the traffic counter immediately, click the **Restart Counter Now** button.
8. Click the **Apply** button.

   Your settings are saved.

   The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see View the Internet traffic volume and statistics on page 128.

Restrict Internet traffic by volume

You can record and restrict traffic by volume in MB. This is useful when your ISP measures your traffic in volume.

To record and restrict the Internet traffic by volume:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
6. Select the **Traffic volume control by** radio button.
7. From the corresponding menu, select an option:

   - **Download only**: The restriction is applied to incoming traffic only.
   - **Both directions**: The restriction is applied to both incoming and outgoing traffic.
8. In the **Monthly limit** field, enter how many MBytes (MB) per month are allowed.
9. If you use a session-based connection type and want to round up the measured data volume to a particular amount for each connection even when you use less, enter the data volume in MB in the **Round up data volume for each connection by** field.
10. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
11. In the Traffic Control section, enter a value in MB to specify when the router issues a warning message before the monthly limit in volume is reached.

    This setting is optional. The router issues a warning when the balance falls below the volume that you enter. By default, the value is 0 and no warning message is issued.
12. Select one or more of the following actions to occur when the limit is reached:

    - **Turn the Internet LED to flashing amber**: This setting is optional. When the traffic limit is reached, the Internet LED blinks amber.
    - **Disconnect and disable the Internet connection**: This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.
13. Click the **Apply** button.

    Your settings are saved.

    The Internet Traffic Statistics section helps you to monitor data traffic. For more information, see View the Internet traffic volume and statistics on page 128.

Restrict Internet traffic by connection time

If you connect to the Internet with a session-based connection type, you can record and restrict traffic by connection time. This is useful when your ISP measures your connection time.

To record and restrict the Internet traffic by connection time:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
6. Select the **Connection time control** radio button.
7. In the **Monthly limit** field, enter how many hours per month are allowed.
8. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
9. In the Traffic Control section, enter a value in minutes to specify when the router issues a warning message before the monthly limit in hours is reached.

   This setting is optional. The router issues a warning when the balance falls under the number of minutes that you enter. By default, the value is 0 and no warning message is issued.
10. Select one or more of the following actions to occur when the limit is reached:

    - **Turn the Internet LED to flashing amber**: This setting is optional. When the traffic limit is reached, the Internet LED blinks amber.
    - **Disconnect and disable the Internet connection**: This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.
11. Click the **Apply** button.

    Your settings are saved.

    The Internet Traffic Statistics section helps you to monitor data traffic. For more information, see View the Internet traffic volume and statistics on page 128.

View the Internet traffic volume and statistics

If you enabled the traffic meter (see Start the traffic meter without traffic volume restrictions on page 125), you can view the Internet traffic volume and statistics.

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

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

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

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

   The Traffic Status pop-up window displays.

Unblock the traffic meter after the traffic limit is reached

If you configured the traffic meter to disconnect and disable the Internet connection after the traffic limit is reached, you cannot access the Internet until you unblock the traffic meter.

CAUTION: If your ISP set a traffic limit, your ISP might charge you for the overage.

To unblock the traffic meter:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Traffic Meter page displays.
5. In the Traffic Control section, clear the **Disconnect and disable the Internet connection** check box.
6. Click the **Apply** button.

   Your settings are saved.

Set the NTP server

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

To set the NTP server:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > NTP Settings**.

   The NTP Settings page displays.
5. Select an NTP server radio button:

- **Use the default NETGEAR NTP server**: Use the preset NETGEAR NTP server.
- **Set your preferred NTP server**: Enter the name or IP address of your preferred server.

6. If you select the **Set your preferred NTP server** radio button, enter the NTP server domain name or IP address in the field below the radio button.
7. Click the **Apply** button.

   Your settings are saved.

Set your time zone and daylight saving time

To set your time zone and daylight saving time:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > NTP Settings**.

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

   Your settings are saved.

Set up the router as a WiFi access point

You can set up the router to run as an access point (AP) on the same local network as another router. When you set up the router as an AP, some of its router features are disabled so that they do not interfere with the router features of the other router.

NOTE: To use AP mode and keep the ability to access to the router web interface, connect using an Ethernet cable from your router's Internet port to a LAN port on your existing network.

To set up the router as an AP:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Router / AP Mode**.

   The Router / AP Mode page displays.
5. Select the **AP Mode** radio button.

   The page adjusts.
6. Select an IP address setting:

   - **Get dynamically from existing router**: The other router on the network assigns an IP address to this router while it is in AP mode.
   - **Use fixed IP address (not recommended)**: Use this setting if you want to manually assign a specific IP address to this router while it is in AP mode. Using this option effectively requires advanced network experience.
7. Click the **Apply** button.

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

Return the router to router mode

By default, your router is set to router mode. If you changed the mode to access point mode (AP mode), you can change the mode back to router mode.

To return the router to router mode:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Router / AP Mode**.

   The Router / AP Mode page displays.
5. Select the **Router Mode** radio button.

   The page adjusts.
6. Click the **Apply** button.

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

Manage LED blinking or turn off LEDs

You can disable or enable LED blinking. You can also turn off the LEDs.

NOTE: These instructions are for disabling or enabling LEDs from the router web interface. You can also press the **LED On/Off** button on the front of the router.

To manage LED blinking or turn off the LEDs:

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

A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > LED Control Settings**.

   The LED Control Settings page displays.

5. Select a radio button:

   - **Enable blinking on Internet LED, LAN LED, Wireless LED, and USB LED when data traffic is detected**: Allows standard LED behavior. This setting is enabled by default.
   - **Turn off all LEDs except Power LED**: All the LEDs, except the Power LED, are turned off.

6. Click the **Apply** button.

   Your settings are saved.

Connect to your router with Anywhere Access

The Anywhere Access feature on the Nighthawk app allows you to connect to your router when you're away from home and change its settings. Before you can use the Anywhere Access feature on the Nighthawk app, you must update your router's firmware and download the latest Nighthawk app for your mobile device.

For more information about how to update your router's firmware, see Update the router firmware on page 110.

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

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 current configuration and reset the router to factory default settings.

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

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

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

Use the Reset button

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

To reset the router to factory default settings:

1. On the back of the router, locate the **Reset** button.
2. Using a straightened paper clip, press and hold the **Reset** button for at least 10 seconds.
3. Release the **Reset** button.

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

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

Erase the settings

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

To erase the settings:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > Administration > Backup Settings**.

   The Backup Settings page displays.
5. Click the **Erase** button.

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

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

10

Share a USB Storage Device Attached to the Router

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

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

The chapter contains the following sections:

- USB device requirements
- Connect a USB storage device to the router
- Display network folders on a storage device
- Access a storage device connected to the router
- Manage access to a USB storage device
- Enable FTP access within your network
- Change a network folder on a USB storage device
- Add a network folder on a USB storage device
- Safely remove a USB storage device
- Change the media server settings or rescan media files

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

USB device requirements

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

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

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

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

Connect a USB storage device to the router

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

To connect a USB device:

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

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

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

Display network folders on a storage device

You can display network folders on a storage device that is connected to the router.

To display network folders:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The USB Storage (Basic Settings) page displays.

   The Available Networks Folder section displays the following information:

   - **Share Name**: If only one USB device is connected, the default share name is USB_Storage.

     You can click the name or you can type it in the address field of your web browser. If Not Shared is shown, the default share was deleted and no other share for the root folder exists.
   - **Read Access**: The read access permission on the network folder. All–no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the router.
   - **Write Access**: The write access permission on the network folder. All–no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the router.
   - **Folder Name**: The full path of the network folder
   - **Volume Name**: The volume name from the storage devic
   - **Total Space and Free Space**: The capacity and available space the storage device

Access a storage device connected to the router

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

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

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

1. Connect a USB storage device to a USB port on your router.
2. If your USB storage device uses a power supply, connect it.

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

   When you connect the USB storage device to the router's port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers on your local area network (LAN).
3. On a Windows-based computer that is connected to the network, select **Start > Run**.
4. Enter **\\readyshare** in the dialog box.
5. Click the **OK** button.

   A window automatically opens and displays the files and folders on the USB storage device.

Map a USB device to a Windows network drive

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

1. Connect a USB storage device to a USB port on your router.
2. If your USB storage device uses a power supply, connect it.

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

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

3. On a Windows-based computer that is connected to the network, select **Start > Run**.
4. Enter **\\readyshare** in the dialog box.
5. Click the **OK** button.

   A window automatically opens and displays the USB storage device.
6. Right-click the USB device and select **Map network drive**.

   The Map Network Drive window opens.
7. Select the drive letter to map to the new network folder.
8. Click the **Finish** button.

   The USB storage device is mapped to the drive letter that you specified.
9. To connect to the USB storage device as a different user, select the **Connect using different credentials** check box, click the **Finish** button, and do the following:

   a. Type the user name and password.
   b. Click the **OK** button.

Access a storage device connected to the router from a Mac

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

To access the device from a Mac:

1. Connect a USB storage device to a USB port on your router.
2. If your USB storage device uses a power supply, connect it.

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

   When you connect the USB storage device to the router's port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers on your local area network (LAN).
3. On a Mac that is connected to the network, open the Finder, then select **Go > Connect to Server**.

   The Connect to Server window opens.
4. In the **Server Address** field, enter **smb://readyshare**.

5. When prompted, select the **Guest** radio button.
6. Click the **Connect** button.

   A window automatically opens and displays the files and folders on the USB storage device.

Manage access to a USB storage device

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

- **Access methods from within your network**:
  - **Windows Network/Mac File Sharing**: Access is enabled by default and no password is required. To access the USB storage device within your network, type **\\readyshare**.
  - **HTTP**: Access is enabled by default and no password is required. To access the USB storage device within your network, type **http://readyshare.routerlogin.net/shares**. You can also click the link that is shown in the Link column.

    The fixed port number is 80.
  - **FTP**: Access is disabled by default. If you enable this feature, by default, no password is required. To access the USB storage device within your network and download or upload files, type **ftp://readyshare.routerlogin.net/shares**. You can also click the link that is shown in the Link column.

    The fixed port number is 21.
- **Remote access methods** :
  - **HTTPS (via Internet)**: Access is disabled by default. If you enable this feature, by default, a password is required. To access the USB storage device remotely over the Internet, type **https://**<*public IP address*>**/shares**. <*public IP address*> is the external or public IP address that is assigned to the router (for example, 203.0.113.102). You can also click the link that is shown in the Link column.

    This feature supports file downloading only. The default port is number 443, which you can change.
  - **FTP (via Internet)**: Access is disabled by default. If you enable this feature, by default, a password is required. To access the USB storage device remotely over the Internet, type **ftp://**<*public IP address*>**/shares**. <*public IP address*> is the external or public IP address that is assigned to the router (for example, 203.0.113.102). You can also click the link that is shown in the Link column.

This feature supports both file uploading and file downloading. The default port is number 21, which you can change.

NOTE: For access from outside your network, we highly recommend that you do *not* disable password protection.

For information about setting up Dynamic DNS (DDNS), which ensures consistent public access, see Use Dynamic DNS to Access a USB Storage Device From the Internet on page 148. If you set up DDNS, you can also type a URL domain name. For example, if your domain name is MyName and you use the NETGEAR DDNS service, you can type https://MyName.mynetgear.com or ftp://MyName.mynetgear.com to access the USB device over the Internet.

To manage the USB storage device access settings:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > USB Functions > Advanced Settings**.

   The USB Storage (Advanced Settings) page displays.
5. To set a name for the workgroup that the USB device or devices are members of, in the **Workgroup** field, type a name.

   By default, the name is Workgroup. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows. If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here.
6. For any access method, enable or disable access:
   - **Allows access**: Select the associated **Enable** check box.
   - **Prevent access**: Clear the associated **Enable** check box.
7. For any access method, to require access with the same password that you set the first time that you logged in to the router, select the associated **Admin Password Protection** check box.

   NOTE: We strongly recommend that you enable admin password protection to secure your ReadySHARE data.

To remove the password requirement, clear the associated **Admin Password Protection** check box.

8. Click the **Apply** button.

   Your settings are saved.

Enable FTP access within your network

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

For information about setting up FTP access through the Internet so that you can remotely access the storage device attached to your router, see Set up FTP access through the Internet on page 152.

To enable FTP access within your network:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > USB Functions > Advanced Settings**.

   The USB Storage (Advanced Settings) page displays.
5. Select the **FTP** check box.
6. Click the **Apply** button.

   Your settings are saved.

Change a network folder on a USB storage device

By default, when you connect a USB storage device to a router USB port, the entire device is shared. You can change the network folder to limit access to specific files or folders.

To change a network folder on a USB storage device:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > USB Functions > Advanced Settings**.

   The USB Storage (Advanced Settings) page displays.
5. Scroll down to the Available Network Folders section and select the USB storage device.

   If a single device is attached to the USB port, the radio button for the device is automatically selected.
6. Click the **Edit** button.

   The Edit Network Folder window opens.
7. Change the settings in the fields as needed.

   For more information about the settings, see Add a network folder on a USB storage device on page 145.
8. Click the **Apply** button.

   Your settings are saved.

Add a network folder on a USB storage device

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

To add a network folder on a USB storage device:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > USB Functions > Advanced Settings**.

   The USB Storage (Advanced Settings) page displays.
5. Scroll down to the Available Network Folders section and select the USB storage device.

   If a single device is attached to the USB port, the radio button for the device is automatically selected.
6. Click the **Create Network Folder** button.

   The Create Network Folder pop-up window displays.

   If this pop-up window does not display, your web browser might be blocking pop-ups. If it is, change the browser settings to allow pop-ups.
7. From the **USB Device** menu, select the USB drive.

   NOTE: We recommend that you do not attach more than one drive to one USB port (for example, through a USB hub).
8. Click the **Browse** button and in the Folder field, select the folder.
9. In the **Share Name** field, type the name of the share.
10. From the **Read Access** menu and the **Write Access** menu, select the security settings that you want.

    All–no password (the default) allows all users to access the network folder. The other option is that only the admin user is allowed access to the network folder. The password for admin is the same one that you use to log in to the router.

11. Click the **Apply** button.

    The folder is added on the USB storage device.
12. Click the **Close Window** button.

    The window closes.

Safely remove a USB storage device

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

To safely remove a USB storage device:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The USB Storage (Basic Settings) page displays.
5. Click the **Safely Remove USB Device** button.

   This takes the device offline.
6. Physically disconnect the USB storage device.

Change the media server settings or rescan media files

By default, the router functions as a Digital Living Network Alliance (DLNA) media server, which lets you view movies and photos on DLNA/UPnP AV-compliant media players, such as TVs and game consoles.

To change the media server settings or rescan media files:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.
4. Select **ADVANCED > USB Functions > Media Server**.

   The Media Server (Settings) page displays.
5. To enable or disable the media server, select or clear the **Enable DNLA Media Server** check box.

   By default, the media server is enabled, allowing the router to function as a DNLA media server.
6. To rescan media files immediately, click the **Rescan media files** button.

   The router automatically scans for media files whenever new files are added to your ReadySHARE USB storage device. Only a shared folder for which the read access settings are All – no password can be scanned for media files.
7. Click the **Apply** button.

   Your settings are saved.
8. To change the name of the media server, click the **Edit** button.

   The Device Name page displays. The device name is the router's default device name, which is based on its model number. This device name displays in the file manager when you browse your network.

   Do the following:

   a. Type a new name in the **Device Name** field.

   b. Click the **Apply** button.

      Your changes are saved.

11

Use Dynamic DNS to Access a USB Storage Device From the Internet

With Dynamic DNS (DDNS), you can use the Internet to access a USB device that's connected to a USB port on the router when you're not home.

This chapter contains the following sections:

- Set up and manage Dynamic DNS
- Your personal FTP server
- Set up HTTPS access through the Internet
- Access a USB storage device through the Internet

Set up and manage Dynamic DNS

Internet service providers (ISPs) assign numbers called IP addresses to identify each Internet account. Most ISPs use dynamically assigned IP addresses. This means that the IP address can change at any time. You can use the IP address to access your network remotely, but most people don't know what their IP addresses are or when this number changes.

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

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

Set up a new Dynamic DNS account

If you do not yet have a Dynamic DNS (DDNS) account, NETGEAR provides you the opportunity to set up a free account.

To set up DDNS and register for a free NETGEAR account:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select **NETGEAR**.

   You can select another service provider.
7. Select the **No** radio button.
8. In the **Host Name** field, type the name that you want to use for your URL.

The host name is the left-most part of a domain name. Your free domain name URL starts with the host name that you specify and ends with mynetgear.com. For example, specify *MyName*.mynetgear.com.

9. In the **Email** field, type the email address that you want to use for your account.
10. In the **Password (6-32 characters)** field, type the password that you want to use for your account.
11. Agree to the terms of service and the privacy policy.
12. Click the **Register** button.

Use a Dynamic DNS account that you already have

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

To set up DDNS if you already have an account:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select your provider.
7. Select the **Yes** radio button.

   The page adjusts and displays the **Show Status**, **Cancel**, and **Apply** buttons.
8. In the **Host Name** field, type the host name that you have registered.
9. In the **Email** field, type the email address for your account.
10. In the **Password (6-32 characters)** field, type the password for your DDNS account.
11. Click the **Apply** button.

Your settings are saved.

12. To verify that your DDNS service is enabled for the router, click the **Show Status** button.

    A message displays the DDNS status.

Manage your existing NETGEAR or No-IP Dynamic DNS account

You can manage the settings for your existing NETGEAR or No-IP Dynamic DNS (DDNS) account, or reset your password for the DDNS account.

To manage your DynDNS account, visit the DynDNS website.

To manage your existing NETGEAR or No-IP DDNS account or reset the password for the DDNS account:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Dynamic DNS page displays.
5. Select the **Yes** radio button.
6. To manage your DDNS account, click the **click here** link next to *To manage your DDNS account*, and sign in to your account.
7. To reset the password for your DDNS account, click the **click here** link next to *Forgot your password*, enter your email address, and click the **Reset** button.
8. Click the **Apply** button.

   Your settings are saved.

Your personal FTP server

With your customized free URL, you can use FTP to access your network through Dynamic DNS when you aren't home. To set up your FTP server, you must register for a NETGEAR Dynamic DNS (DDNS) service account and specify the account settings. See Set up a new Dynamic DNS account on page 149.

Set up your personal FTP server: Overview of steps

To set up your personal account:

1. Get your NETGEAR Dynamic DNS domain name.

   For more information, see Set up a new Dynamic DNS account on page 149.
2. Make sure that your Internet connection is working.

   Your router must use a direct Internet connection. You router cannot connect to *another* router to access the Internet.
3. Connect a USB storage device to the router.

   For more information, see Connect a USB storage device to the router on page 137.
4. Set up remote FTP access to the router.

   For more information, see Set up FTP access through the Internet on page 152.

After you have set up remote FTP access, you can use it to access your router from a remote computer with Internet access, using ftp://*yourname*.mynetgear.com.

Set up FTP access through the Internet

To set up FTP access through the Internet:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > USB Functions > Advanced Settings**.

   The USB Storage (Advanced Settings) page displays.
5. Select the **FTP (via Internet)** check box.

   The default port is number 21. Password protection is enabled by default. We highly recommend that you keep password protection enabled.
6. Click the **Apply** button.

   Your settings are saved.

   The link that lets you access the device over the Internet is ftp://*public-ip-address*/shares. In this link, *public-ip-address* represents one of the following:
   - The IP address that is assigned to the router's Internet port. You can view this IP address on the ADVANCED Home page.
   - If you set up a DDNS account, the router's DNS name, for example, *yourname.mynetgear.com*.
7. To limit read and write access of the attached USB storage device to the admin user, select the device in the Available Network Folders section.

   If only one device is connected, it is automatically selected.
8. Click the **Edit** button.

   The Edit page displays.
9. From the **Read Access** menu, select **admin**.
10. From the **Write Access** menu, select **admin**.
11. Click the **Apply** button.

    Your settings are saved.

Set up HTTPS access through the Internet

To set up HTTPS access through the Internet:

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

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

The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

The BASIC Home page displays.

4. Select **ADVANCED > USB Functions > Advanced Settings**.

   The USB Storage (Advanced Settings) page displays.

5. Select the **HTTPS (via Internet)** check box.

   The default port is number 443. Password protection is enabled by default. We highly recommend that you keep password protection enabled.

6. Click the **Apply** button.

   Your settings are saved.

   The link that lets you access the device over the Internet is https://*public-ip-address*/shares. In this link, *public-ip-address* represents one of the following:

   - The IP address that is assigned to the router's Internet port. You can view this IP address on the ADVANCED Home page.
   - If you set up a DDNS account, the router's DNS name, for example, *yourname.mynetgear.com*.

7. To limit read and write access of the attached USB storage device to the admin user, select the device in the Available Network Folders section.

   If only one device is connected, it is automatically selected.

8. Click the **Edit** button.

   The Edit page displays.

9. From the **Read Access** menu, select **admin**.
10. From the **Write Access** menu, select **admin**.
11. Click the **Apply** button.

    Your settings are saved.

Access a USB storage device through the Internet

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

To access a device from a remote computer:

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

   The link that lets you access the device over the Internet is https://*public-ip-address*/shares. In this link, *public-ip-address* represents one of the following:

   - The IP address that is assigned to the router's Internet port. You can view this IP address on the ADVANCED Home page.
   - If you set up a DDNS account, the router's DNS name, for example, *yourname.mynetgear.com*.

     For information about using Dynamic DNS (DDNS), see Set up and manage Dynamic DNS on page 149.
3. If password protection is enabled (which it is by default), type your admin password.

   You can now access your storage devices.

12

Use OpenVPN to Access Your Network

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

The chapter contains the following sections:

- About VPN connections
- LAN IP addressing in VPN networks
- Enable OpenVPN service on the router
- Install OpenVPN software on a VPN client
- Use VPN to access your Internet service at home

About VPN connections

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

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

- Log in to the router to enable and configure OpenVPN (see Enable OpenVPN service on the router on page 158).
- Install OpenVPN client software and configuration files on your device from which you want to use VPN (see Install OpenVPN software on a VPN client on page 159).
- Run the OpenVPN client software on your device when you want to use a VPN connection.

Enabling OpenVPN on your router allows VPN connections between the router and a client, for example your laptop when you are away from home. The router provides the VPN service and the laptop is the VPN client. Traffic between the router and the laptop is encrypted. You can also use a VPN connection to remotely access a USB storage device attached to your router without enabling the FTP or HTTPS (via Internet) functions.

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

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

- To use a DDNS service, register for a DDNS account with a host name. You use the host name to access your network. The router supports these DDNS accounts: NETGEAR, No-IP, and Dyn. For more information, see Set up and manage Dynamic DNS on page 149.
- If your Internet service provider (ISP) assigned a static WAN IP address that never changes, the VPN can use that IP address to connect to your home network.

LAN IP addressing in VPN networks

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

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

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

For information about changing the LAN settings on the router, see Change the LAN IP address settings or RIP settings on page 88.

Enable OpenVPN service on the router

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

To enable OpenVPN service:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The VPN Service page displays.

   NOTE: The OpenVPN configuration software packages that you can download on the page are for the VPN client devices (see Install OpenVPN software on a VPN client on page 159).
5. Select the **Enable VPN Service** check box.

   We recommend that you use the default TUN mode and TAP mode settings. (These settings determine how VPN information is transferred.) If you know that you need other settings, you can change the TUN mode and TAP mode settings, but you must do so *before* you download and install the OpenVPN configuration software packages on client devices (see Install OpenVPN software on a VPN client on page 159).
6. To change the TUN mode settings, do the following:
   - To change the TUN mode service type, select the **UDP** or **TCP** radio button.

The default protocol for TUN mode is UDP.

- To change the TUN mode service port, type the port number that you want to use in the field.

  The default port number for TUN mode is 12973. The TUN port number is used in the `.ovpn` file of the OpenVPN configuration software package for Mac and non-Windows clients.

7. To change the TAP mode settings, do the following:
   - To change the TAP mode service type, select the **UDP** or **TCP** radio button.

     The default protocol for TAP mode is UDP.
   - To change the TAP mode service port, type the port number that you want to use in the field.

     The default port number for TAP mode is 12974. The TAP port number is used in the `.ovpn` file of the OpenVPN configuration software package for Windows clients.
8. Click the **Apply** button.

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

Install OpenVPN software on a VPN client

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

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

- Download and install the application software from the link that is provided in each client-specific section.
- Download and install the configuration files from the router as described in each client-specific section. The configuration files provide the correct router configuration information for the client utility. You must download the configuration files *after* you enable and configure OpenVPN service on the router (see Enable OpenVPN service on the router on page 158).

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

Install OpenVPN software on a Windows-based computer

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

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

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

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

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

   For more information about the VPN configuration for the router, see Enable OpenVPN service on the router on page 158.

9. Click the **For Windows** button to download the router's OpenVPN configuration files to your Windows-based computer.
10. Unzip the OpenVPN configuration files and copy them to the **config** sub-folder in your OpenVPN client utility installation folder.

    You can also import the unzipped `.ovpn` configuration file from the OpenVPN client user interface.
11. Modify the VPN interface name to **NETGEAR-VPN**:

    a. If your computer is running Windows 10 or newer, select **Start > Settings > Network & Internet > Change adapter options**.

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

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

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

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

You can now open a VPN tunnel to the router.

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

Install OpenVPN software on a Mac

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

To download and install the OpenVPN Connect utility and OpenVPN configuration files on a Mac:

1. To download the OpenVPN Connect utility on your Mac, visit https://openvpn.net/client-connect-vpn-for-mac-os/.
2. Download and install the OpenVPN Connect utility on your Mac.

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

The BASIC Home page displays.

6. Select **ADVANCED > Advanced Setup > VPN Service**.

   The VPN Service page displays.

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

   For more information about the VPN configuration for the router, see Enable OpenVPN service on the router on page 158.

8. Click the **For non-Windows** button to download the router's OpenVPN configuration files to your Mac.
9. Unzip the OpenVPN configuration file and import the unzipped `.ovpn` file from the OpenVPN client user interface.

You can now open a VPN tunnel to the router.

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

Install OpenVPN software on an iOS device

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

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

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

   A login window displays.

4. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > VPN Service**.

   The VPN Service page displays.

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

   For more information about the VPN configuration for the router, see Enable OpenVPN service on the router on page 158.

7. Click the **For Smart Phone** button to download the router's OpenVPN configuration file to your computer or iOS device.

   If you download the configuration file to your computer, unzip the `.ovpn` file, and send it to your iOS device.

8. On your iOS device, do the following:
   a. Open the OpenVPN Connect app.
   b. Import the `.ovpn` configuration file.

      NOTE: If you sent the configuration file from a computer, you should see the file listed. If you downloaded the file directly to your iOS device, locate the download folder and share the unzipped `.ovpn` configuration file with the OpenVPN Connect app.

You can now open a VPN tunnel to the router.

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

Install OpenVPN software on an Android device

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

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

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

   A login window displays.

4. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > VPN Service**.

   The VPN Service page displays.

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

For more information about the VPN configuration for the router, see Enable OpenVPN service on the router on page 158.

7. Click the **For Smart Phone** button to download the router's OpenVPN configuration file to your computer or Android device.

   If you download the configuration file to your Android device, unzip the file. If you download the configuration files to your computer, unzip the files, and send them to your Android device.

8. On your Android device, open the OpenVPN Connect app and import the `.ovpn` file.

You can now open a VPN tunnel to the router.

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

Use VPN to access your Internet service at home

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

Your router lets you use a VPN connection to access your own Internet service when you're away from home. You might want to do this to encrypt the data to and from your device so that any data intercepted by a third party cannot read the data. You might also want to use a VPN connection if you travel to a geographic location that doesn't support all the Internet services that you use at home. For example, your Netflix account might work at home but not in a different country.

NOTE: The data sent between your device and your router is encrypted by the VPN, but the data exchanged between your router and the public Internet is not protected by the VPN service.

Allow VPN client Internet access in the router

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

To allow VPN clients to use your home Internet service:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

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

   For more information about the VPN configuration for the router, see Enable OpenVPN service on the router on page 158.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **All sites on the Internet & Home Network** radio button.

   When you access the Internet with the VPN connection, instead of using a local Internet service, you use the Internet service from your home network.
7. Click the **Apply** button.

   Your settings are saved.

Block VPN client Internet access in the router

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

To allow VPN clients to access only your home network and block them from using the Internet service for your home network:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

   The BASIC Home page displays.

4. Select **ADVANCED > Advanced Setup > VPN Service**.

   The VPN Service page displays.

5. Make sure that the **Enable VPN Service** check box is selected.

   For more information about the VPN configuration for the router, see Enable OpenVPN service on the router on page 158.

6. Scroll down to the Clients will use this VPN connection to access section, and select the **Home Network only** radio button.

   This is the default setting. The VPN connection is only to your home network, not to the Internet service for your home network.

7. Click the **Apply** button.

   Your settings are saved.

13

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
- Manage port triggering

Manage port forwarding to a local server

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 85).

Forward incoming traffic to a local server

You can forward traffic for a default service or application to a server 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 must provide the service.

   The server computer must always receive the same IP address.
3. Assign the server computer a reserved IP address.

   See Manage reserved LAN IP addresses on page 91.
4. Launch a web browser from a computer or mobile device that is connected to the router network.
5. Enter **http://www.routerlogin.net**.

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The Port Forwarding / Port Triggering page displays.
8. Leave the **Port Forwarding** radio button selected as the service type.
9. From the **Service Name** menu, select the service or application.

If the service or application that you want to add is not in the list, create a port forwarding rule with a custom service or application (see Add a custom port forwarding service or application on page 169).

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

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

Add a custom port forwarding 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 custom service or application that you can then select for a port forwarding rule.

To add a custom service or application:

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

   You can usually find this information by contacting the publisher of the application or user groups or news groups.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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. Leave the **Port Forwarding** radio button selected as the service type.
7. Click the **Add Custom Service** button.

   The Ports - Custom Services page displays.
8. In the **Service Name** field, enter a descriptive name.
9. From the **Protocol** menu, select the protocol.

   If you are unsure, select **TCP/UDP**.
10. In the **External Port Range** field, enter the port range.

You can specify ports and port ranges divided by commas, for example: 30, 50–60, 65500–65510.

11. Specify the internal ports by one of these methods:
    - Leave the **Use the same port range for Internal port** check box selected.
    - Type the port numbers in the **Internal Port Range** field.

      You can enter a port range and fixed ports in one rule, for example: external (30–50, 78, 100–102), internal (40–60, 99, 200–202). With this rule, external ports 30–50 are forwarded to internal ports 40–60.
12. In the **Internal IP address** field, type the IP address or select the radio button for an attached device listed in the table.
13. Click the **Apply** button.

    Your settings are saved. The service or application is now in the list on the Port Forwarding / Port Triggering page.

Change a port forwarding rule

You can change an existing port forwarding rule.

To change a port forwarding rule:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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. Leave the **Port Forwarding** radio button selected as the service type.
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 custom port forwarding service or application on page 169.

9. Click the **Apply** button.

   Your settings are saved. The changed rule displays in the table on the Port Forwarding / Port Triggering page.

Remove a port forwarding rule

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

To remove a port forwarding rule:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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. Leave the **Port Forwarding** radio button selected as the service type.
6. In the table, select the radio button for the service or application name.
7. Click the **Delete Service** button.

   Your settings are saved. 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 a fixed IP address using DHCP address reservation.

In this example, your router always gives your web server an IP address of 192.168.1.33.

2. On the Port Forwarding / Port Triggering page, configure the router to forward the HTTP service to the local address of your web server at 192.168.1.33.

   HTTP (port 80) is the standard protocol for web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and specify that name on the Dynamic DNS page of the router.

   Dynamic DNS makes it much easier to access a server from the Internet because you can enter the name in the web browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

How the router implements the port forwarding rule

The following sequence shows the effects of a port forwarding rule in which your router always gives your web server an IP address of 192.168.1.33:

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 192.168.1.33 and sends the message to that computer.
4. Your web server at IP address 192.168.1.33 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

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 through that port, the router saves the IP address of the computer that sent the traffic. The router temporarily opens the incoming port or ports that you specify in your rule and forwards that incoming traffic to that destination.

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

NOTE: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance, enable Universal Plug N Play (UPnP). See Improve network connections with Universal Plug and Play on page 107.

Add a port triggering rule

The router does not include a predefined list of default services and applications for port triggering rules. You must define a custom service or application for each port triggering rule. After you add the rule, it is automatically enabled.

To add a port triggering rule:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 Services page displays.

7. Specify the following settings:
   - **Service Name**: Enter the name of the custom service or application.
   - **Service User**: From the **Service User** menu, select **Any**, or select **Single address** and enter the IP address of one computer:
     - **Any**: This is the default setting and allows any computer on the Internet to use this service or application.
     - **Single address**: Restricts the service or application to a particular computer. Enter the IP address in the fields, which become available with this selection from the menu.
   - **Service Type**: Select the protocol (**TCP** or **UDP**) that is associated with the service or application.
   - **Triggering Port**: Enter the number of the outbound traffic port that will trigger opening of the inbound ports when traffic is sensed.
   - **Connection 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 service or application is added to the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

   By default, the rule for the new service or application is enabled.

Change a port triggering rule

You can change an existing port triggering rule.

To change a port triggering rule:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 rule.
7. Click the **Edit Service** button.

   The Port Triggering Services page displays.

8. Change the settings.

   For information about the settings, see Add a port triggering rule on page 173.

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 device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 rule.
7. Click the **Delete Service** button.

   Your settings are saved. The rule is removed from the Port Triggering Portmap Table.

Set the time-out period for port triggering

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

To specify the time-out for port triggering:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. 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 an individual port triggering rule

By default, port triggering is enabled. You can disable port triggering temporarily without removing any port triggering rules (see Disable port triggering on page 177). You can also keep port triggering enabled and disable an individual port triggering rule.

To disable an individual port triggering rule:

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

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

The user name is **admin**. The password is the one that you specified when you set up your router. 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, clear the check box for the rule that you want to disable.
7. Click the **Apply** button.

   Your settings are saved. The router does not apply the rule that you disabled.

Disable port triggering

By default, port triggering is enabled. You can disable port triggering temporarily without removing any port triggering rules. For information about disabling an individual port triggering rule, see Disable an individual port triggering rule on page 176.

To disable port triggering:

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

   A login window displays.

3. Enter the router admin user name and password.

   The user name is **admin**. The password is the one that you specified when you set up your router. 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.
7. Click the **Apply** button.

   Your settings are saved. The router does not apply port triggering rules even if you specified them.

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 reaches its port triggering time-out period due to 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.

14

Troubleshooting

This chapter provides information to help you diagnose and solve problems you might experience with your router. If you do not find the solution here, check the NETGEAR support site at netgear.com/support for product and contact information.

The chapter contains the following sections:

- Quick tips
- Reboot the router from its router web interface
- Troubleshoot with the LEDs
- You cannot log in to the router
- You cannot access the Internet
- Troubleshoot Internet browsing
- Changes are not saved
- Troubleshoot WiFi connectivity
- Troubleshoot your network using the ping utility

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. Disconnect all devices from the modem.
3. Turn off the router.
4. Plug in the modem and turn it on.
5. Wait two minutes.
6. Reconnect the router to the modem.

   Do not connect any other devices to the modem.
7. Turn on the router.
8. Wait two minutes.

   When your network is back up, you can reconnect other devices to the modem.

Check the power adapter and Ethernet cable connections

If the router does not start, make sure that the power adapter cable is securely plugged in.

If the Internet connection or LAN connections do not function, make sure that the Ethernet cables are securely plugged in.

The Internet LED on the router is lit if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.

If one or more powered-on computers are connected to the router by an Ethernet cable, the Ethernet LAN LED lights.

Check the WiFi settings

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

the router and the computer or mobile device must match exactly. WiFi passwords are case sensitive.

If you set up an access control list that blocks all new devices from connecting, you must add the MAC address of each computer and mobile device to the router's access control list.

Check the network settings

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

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

Reboot the router from its router web interface

You or NETGEAR technical support can reboot the router from its router 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 router web interface:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The ADVANCED Home page displays.

5. Click the **Reboot** button.
   A confirmation pop-up window displays.
6. Click the **OK** button.
   The router reboots.

Troubleshoot with the LEDs

By default, the router uses standard LED settings.

Standard LED behavior when the router is powered on

After you turn on power to the router, verify that the following sequence of events occurs:

1. When power is first applied, verify that the Power LED is lit.
2. After about two minutes, verify the following:
   - The 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

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.

Power LED stays solid amber or blinking amber

When the router is turned on, the Power LED lights solid amber during the boot up, and then turns solid white when the startup is done. If the Power LED stays solid amber or blinking amber, or no other LEDs are lit, this indicates a fault within the router.

NOTE: The Power LED is blinking amber temporarily when the firmware is upgrading, or the Reset button was pressed. This is expected behavior.

If the Power LED stays solid amber or blinking amber for more than three minutes *after powering up*, try the following:

- Cycle the power to see if the router recovers.
- Turn off the router, press and hold the **Reset** button, power on the router, and then release the **Reset** button to return the router to its factory settings.

If the Power LED continues to stay amber, the router firmware might be corrupted. This can happen if a firmware update is interrupted, or if the router detects a problem with the firmware. If the error persists, it is likely that a hardware problem exists. For recovery instructions, or help with a hardware problem, contact Technical Support at netgear.com/support.

Internet or Ethernet LAN port LEDs are off

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

- Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.
- Make sure that power is turned on to the connected modem or computer.
- Be sure that you are using the correct cable.

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

WiFi LED is off

A WiFi radio is the component inside your router that broadcasts WiFi signal. Each radio (for example, the 5 GHz radio) has its own WiFi broadcast.

If the WiFi LED stays off, check to see if someone disabled the WiFi radios from the router web interface. 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 or mobile device on your local network, check the following:

- If you are using an Ethernet-connected computer, check the cable connection between the computer and the router.
- If you are using a WiFi-enabled computer or mobile device, check the WiFi connection between the computer or mobile device and the router. Make sure that your computer or mobile device is not connected to a different router or gateway's WiFi network that uses the same network name.
- Make sure that you are using the correct login information. The user name is **admin**. The password is the one thatyou specified when you set up your router. (The default password is **password**.) The user name and password are case-sensitive. Make sure that Caps Lock is off when you enter this information.
- Try quitting the browser and launching it again.
- Make sure that JavaScript is enabled in your browser.
- Make sure that the IP address of your computer or mobile device is in the same subnet as the router. If you are using the recommended addressing scheme, the IP address of your computer or mobile device is in the range of 192.168.1.2 to 192.168.1.254.
- If the IP address of your computer or mobile device is shown as 169.254.x.x, the computer or mobile device could not reach the router's DHCP server and the Windows or Mac operating system generated an IP address itself. Such an autogenerated IP address is in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer or mobile device to the router, and restart your computer or mobile device.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults and disconnect the Ethernet cable from the Internet port. This sets the router's IP address to 192.168.1.1.

  NOTE: If the router is in access point mode and you do not know the IP address that is assigned to it, first try to use an IP scanner application to detect the IP address. (IP scanner applications are available online free of charge.) If you can detect the IP address, you don't need to reset the router to factory default settings. You can also connect the router in access point mode to your existing network using the Internet port, then connect to the access point router and access the router web interface from **http://www.routerlogin.net/**.

- If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services. For example, the router cannot convert ADSL or cable data into Ethernet networking information. Your NETGEAR router does not support such a configuration. You need a modem to connect to your cable, satellite, or xDSL service, and can connect your router to that modem via Ethernet.

NOTE: If you use high-speed fiber Internet service, you might not need a separate modem. Contact your Internet service provider (ISP) for more information.

You cannot access the Internet

If you can access your router but not the Internet, check to see if the router can obtain a Internet IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful using the router web interface.

To check the Internet IP address:

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

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

   The user name is **admin**. The password is the one that you specified when you set up your router. The user name and password are case-sensitive.

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

   The ADVANCED Home page displays.
5. In the Internet Port pane, 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.
6. If your router did not obtain an IP address from your ISP, click **Connection Status**.

   The Connection Status window displays.
7. Click **Release**.

   Your router releases its DHCP lease.
8. Click **Renew**.

   Your router attempts to get 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 180.

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 be experiencing an outage. Try connecting a computer directly to your modem's Ethernet port and accessing the internet. If your computer still can't access the Internet, contact your ISP to troubleshoot your connection.
- Your ISP might require a login program. Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account as the account name on the Internet Setup page.
- If your ISP allows only one Ethernet MAC address to connect to the 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 use your computer's MAC address (see Manually set up the Internet connection on page 30).

If your router obtained an IP address, but your computer does not load any web pages from the Internet, it might be for one or more of the following reasons:

- Your computer or mobile device might not recognize any DNS server addresses.

  Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered DNS addresses during the router's configuration, restart your computer or mobile device and verify the DNS addresses. You can also try removing the DNS addresses that you entered, which lets the router try to get DNS server addresses automatically from your ISP. Make sure that your computer or mobile device is configured to receive DNS server addresses automatically and that you did not manually specify any DNS server addresses in your computer or mobile device.
- The router might not be configured as the TCP/IP gateway on your computer or mobile device.

  Make sure that your computer or mobile device is configured as a DHCP client (for most devices, this is the default setting) so that the computer or mobile device can automatically receive an IP address from the router. If you need to enable the DHCP client on your computer or mobile device, restart the computer or mobile device, and then verify the gateway address.
- You might be running login software that is no longer needed.

  If your ISP provided a program to log you in to the Internet, you no longer need to run that software after installing your router

Troubleshoot Internet browsing

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet, it might be for the following reasons:

- The traffic meter is enabled, and the limit was reached.

  By configuring the traffic meter not to block Internet access when the traffic limit is reached, you can resume Internet access. If your Internet service provider (ISP) sets a usage limit, they might charge you for the overage.
- Your computer or mobile device might not recognize any DNS server addresses.

  Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered DNS addresses during the router's configuration, restart your computer or mobile device, and verify the DNS addresses. Make sure that your computer or mobile device is configured to receive DNS server addresses automatically and that you did not manually specify any DNS server addresses in your computer or mobile device.
- The router might not be configured as the default gateway on your computer or mobile device.

  Make sure that your computer or mobile device is configured as a DHCP client (for most devices, this is the default setting) so that the computer or mobile device can automatically receive an IP address from the router. If you need to enable the DHCP client on your computer or mobile device, restart the computer or mobile device, and then verify the gateway address.

Changes are not saved

If the router does not save the changes that you make in the router web interface, do the following:

- When entering configuration settings, always click the **Apply** button before moving to another page or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. It is possible that the changes occurred, but the old settings might be in the web browser's cache.

Troubleshoot WiFi connectivity

If you are experiencing trouble connecting over WiFi to the router, try to isolate the problem:

- Does the WiFi device that you are using find your WiFi network?

  If not, check the WiFi LED on the router. If it is off, log in to the router web interface and check if the WiFi radio is enabled or disabled.

  If you disabled the router's SSID broadcast, then your WiFi network is hidden and does not display in your WiFi device's scanning list. (By default, SSID broadcast is enabled.)
- Is there another WiFi router, gateway, access point, or extender broadcasting the same network name as your router?

  Make sure that any other WiFi broadcast devices are either turned off or using a different WiFi network name.
- Does your WiFi device support the security that you are using for your WiFi network (WPA3, WPA2, or WPA)?
- 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**. (Be sure to click the **Apply** button if you change settings.)

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

- Is your router too far from your WiFi device or too close? Place your WiFi 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 WiFi device blocking the WiFi signal? Install your router as close to the center of your home as possible. Avoid installing the router in your kitchen, basement, or under stairs. Kitchen appliances and obstructions like walls or floors can create interference that impacts your WiFi performance.

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 troubleshoot a network using the ping utility in your computer or workstation.

Test the LAN path to your router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a Windows-based computer:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   ping www.routerlogin.net
3. Click the **OK** button.

   You see a message like this one:

   ```
   Pinging <IP address > with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

If the path is not functioning correctly, one of the following problems might be occurring:

- Wrong physical connections

  For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.

  Check to see that the appropriate LEDs are lit for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and router.
- Wrong network configuration

  Verify that the Ethernet driver software and TCP/IP software are both installed and configured on your computer.

  Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Test the path from a Windows-based computer to a remote device

To test the path from a Windows-based computer to a remote device:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the Windows Run window, type

   ping -n 10 *<IP address>*

   where *<IP address>* is the IP address of a remote device such as your ISP DNS server.

If the path is functioning correctly, messages display that are similar to those shown in Test the LAN path to your router on page 188.

3. If you do not receive replies, check the following:
   - Check to see that the 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 use the authorized computer's MAC address (see Manually set up the Internet connection on page 30).