

NETGEAR®

User Manual

Nighthawk AC2300 Cybersecurity WiFi Router

Model RS400

July 2019
202-11963-02

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

Support

Thank you for purchasing this NETGEAR product.

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

Contact your Internet service provider for technical support.

Trademarks

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

Compliance and Conformity

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

Contents

Chapter 1 Hardware Setup

- Unpack your router.....10
- Attach the antennas.....10
- LEDs and buttons on the top panel.....11
- Rear panel.....12
- Router label and QR Code label.....13
- Position your router.....14
- Cable your router.....15

Chapter 2 Connect to the Router’s Network and Automatically Set Up the Internet Connection

- Connect to the network.....18
 - Connect to the network using a wired connection.....18
 - Find and connect to the WiFi network.....18
 - WiFi connection using WPS.....18
- Types of logins.....19
- Use a web browser to access the router.....19
 - Use a web browser to set up the router’s Internet connection automatically.....20
 - Log in to the router.....22
- Change the language.....23
- Install and manage your router with the Nighthawk app.....24

Chapter 3 Specify Your Internet Settings

- Use the Internet Setup Wizard.....26
- Manually set up the Internet connection.....26
 - Specify an Internet connection without a login.....26
 - Specify an Internet connection that uses a login and PPPoE service.....28
 - Specify an Internet connection that uses a login and PPTP or L2TP service.....29
- Specify IPv6 Internet connections.....31
 - Requirements for entering IPv6 addresses.....32
 - Use Auto Detect for an IPv6 Internet connection.....32
 - Set up an IPv6 6to4 tunnel Internet connection.....33
 - Set up an IPv6 pass-through Internet connection.....35

- Set up a fixed IPv6 Internet connection.....35
- Set up an IPv6 DHCP Internet connection.....36
- Set up an IPv6 PPPoE Internet connection.....38
- Use Auto Config for an IPv6 Internet connection.....40
- Set up an IPv6 6rd tunnel connection.....41
- Manage the MTU size.....43
 - MTU concepts.....43
 - Change the MTU size.....44

Chapter 4 Control Access to the Internet

- Manage NETGEAR Armor.....46
 - Activate Armor using the Nighthawk app.....46
 - View or change your NETGEAR Armor settings using the Nighthawk app.....46
 - View or change your NETGEAR Armor settings from the Armor portal.....47
 - Sign in to NETGEAR Armor from the router web interface and start your subscription.....47
 - Access the NETGEAR Armor portal from the router web interface.....48
 - Disable or Reenable NETGEAR Armor from the router web interface.....48
- Enable Circle with Disney.....49
 - Enable Circle with Disney using the Nighthawk app.....50
 - Enable Circle with Disney using the Circle app.....50
- Enable access control to allow or block access to the Internet...51
- Manage network access control lists.....52
- Use keywords to block Internet sites.....53
- Delete keywords from the blocked list.....54
- Prevent blocking on a trusted computer.....54
- Block services from the Internet.....55
- Schedule when to block Internet sites and services.....56
- Set up security event email notifications.....57

Chapter 5 Optimize Performance

- Use Dynamic QoS to optimize Internet traffic management.....60
 - Enable Dynamic QoS.....60
 - Enable or disable the automatic QoS database update.....61
 - Manually update the Dynamic QoS database.....61
- Wi-Fi Multimedia Quality of Service.....62
- Improve network connections with Universal Plug and Play.....63
- Enable or disable Smart Connect.....64

Chapter 6 Manage Network Settings

View or change the WAN settings.....	67
Set up a default DMZ server.....	68
Change the LAN TCP/IP settings.....	69
Change the router's device name.....	70
Specify the IP addresses that the router assigns.....	71
Disable the DHCP server feature in the router.....	72
Manage reserved LAN IP addresses.....	73
Reserve an IP address.....	73
Edit a reserved IP address.....	74
Delete a reserved IP address entry.....	75
Set up the router as a WiFi access point.....	75
Set up the router in bridge mode.....	76
Return the router to router mode.....	78
Set up a bridge for a port group or VLAN tag group.....	78
Set up a bridge for a port group.....	79
Set up a bridge for a VLAN tag group.....	80
Manage custom static routes.....	81
Set up a static route.....	82
Edit a static route.....	83
Delete a static route.....	83

Chapter 7 Manage the WiFi Network Settings

Use the WPS Wizard for WiFi connections.....	86
Specify basic WiFi settings.....	86
Change the WiFi password or the WiFi security.....	88
Set up WPA/WPA2 enterprise WiFi security.....	90
Set up WEP legacy WiFi security.....	92
Change the WiFi Mbps settings.....	94
Change the transmission power of the WiFi radios.....	95
Set up a guest WiFi network.....	96
Control the WiFi radios.....	98
Use the WiFi On/Off button.....	99
Enable or disable the WiFi radios.....	99
Set up a WiFi schedule.....	99
Manage WPS settings.....	100
Enable or disable implicit beamforming.....	102
Enable or disable airtime fairness.....	102
Enable or disable MU-MIMO.....	103
Manage advanced WiFi settings.....	104

Chapter 8 Manage Your Router

Update the router firmware.....	107
---------------------------------	-----

- Check for new firmware and update the router.....107
- Manage the firmware update settings.....108
- Manually upload firmware to the router.....108
- Change the admin password.....109
- Enable admin password recovery.....110
- Recover the admin password.....111
- Manage the router configuration file.....111
 - Back up the settings.....112
 - Restore the settings.....112
- View information about the router and the Internet and WiFi settings.....113
- Display the statistics of the Internet port.....114
- Check the Internet connection status.....115
- View and manage logs of router activity.....116
- View devices currently on the network.....117
- Monitor, meter, and control Internet traffic.....118
 - Start the traffic meter without traffic restrictions.....118
 - Restrict Internet traffic by volume.....119
 - Restrict Internet traffic by connection time.....120
 - View the Internet traffic volume and statistics.....121
 - Unblock the traffic meter after the traffic limit is reached.....122
- Set your time zone.....122
- Change the NTP server.....123
- Disable LED blinking or turn off LEDs.....124
- Return the router to its factory default settings.....124
 - Use the Reset button.....125
 - Erase the settings.....125

Chapter 9 Share USB Storage Devices Attached to the Router

- USB device requirements.....128
- Connect a USB storage device to the router.....128
- Access a storage device connected to the router.....129
 - Access a storage device connected to the router from a Windows-based computer.....129
 - Map a USB device to a Windows network drive.....129
 - Access a storage device that is connected to the router from a Mac.....130
- Back up Windows-based computers with ReadySHARE Vault....131
- Enable FTP access within your network.....132
- View network folders on a storage device.....132
- Add a network folder on a USB storage device.....133
- Edit a network folder on a USB storage device.....134
- Approve a USB storage device.....135
- Remotely access a USB device using ReadyCLOUD.....136

Create a ReadyCLOUD account.....136
Register your router with ReadyCLOUD.....137
Safely remove a USB storage device.....138

Chapter 10 Use VPN to Access Your Network

Set up a VPN connection.....140
Manage Dynamic DNS for VPN connections.....140
 Set up a new Dynamic DNS account.....140
 Specify a DNS account that you already created.....141
 Change the Dynamic DNS settings.....142
Enable and configure OpenVPN on the router.....143
Install OpenVPN software.....144
 Install the OpenVPN client utility and VPN configuration files on
 a Windows-based computer.....144
 Install the OpenVPN client utility and VPN configuration files on
 a Mac.....146
 Install the OpenVPN client utility and VPN configuration files on
 an iOS device.....147
 Install the OpenVPN client utility and VPN configuration files on
 an Android device.....148
LAN requirements for VPN connections.....149
Use a VPN tunnel on a Windows-based computer.....149
Use VPN to access your Internet service at home.....150
 Allow VPN clients full Internet access.....150
 Use a VPN tunnel to access your Internet service at home....151
 Block Internet access for VPN clients.....151

Chapter 11 Manage Port Forwarding and Port Triggering Traffic Rules

Manage port forwarding to a local server for services and
applications.....154
 Forward incoming traffic for a default service or application.154
 Add a port forwarding rule for a custom service or
 application.....155
 Change a port forwarding rule.....157
 Remove a port forwarding rule.....157
 Application example: Make a local web server public.....158
 How the router implements a port forwarding rule.....159
Manage port triggering for services and applications.....159
 Add a port triggering rule.....160
 Change a port triggering rule.....161
 Specify the time-out for port triggering.....162
 Disable port triggering.....163
 Remove a port triggering rule.....163

Application example: Port triggering for Internet Relay Chat. 164

Chapter 12 Troubleshooting

Quick tips..... 167

- Sequence to restart your network..... 167
- Check the power adapter and Ethernet cable connections... 167
- Check the WiFi settings..... 167
- Check the network settings..... 167

Troubleshoot with the LEDs..... 168

- Standard LED behavior when the router is powered on..... 168
- Power LED is off or blinking..... 168
- LEDs never turn off..... 168
- Internet or Ethernet LAN port LEDs are off..... 169
- WiFi LEDs are off..... 169

You cannot log in to the router..... 169

Resolve a browser security warning..... 170

- Google Chrome: add a security exception..... 171
- Apple Safari: add a security exception..... 172
- Mozilla Firefox: add a security exception..... 172
- Microsoft Internet Explorer: add a security exception..... 173
- Microsoft Edge: add a security exception..... 174

You cannot access the Internet..... 175

Troubleshoot Internet browsing..... 177

Changes are not saved..... 177

Troubleshoot WiFi connectivity..... 177

Troubleshoot your network using the ping utility..... 178

- Test the LAN path to your router..... 178
- Test the path from a Windows-based computer to a remote device..... 179

Appendix A Supplemental Information

Factory settings..... 182

Technical specifications..... 183

1

Hardware Setup

The NETGEAR Nighthawk AC2300 Cybersecurity WiFi Router Model RS400 comes with NETGEAR Armor built-in and includes a 3-year NETGEAR Armor subscription.

NETGEAR Armor protects your connected home from Internet threats and provides best-in-class anti-virus and data theft protection for all of your smartphones and computers, with an unlimited number of devices covered.

This chapter contains the following sections:

- [Unpack your router](#)
- [Attach the antennas](#)
- [LEDs and buttons on the top panel](#)
- [Rear panel](#)
- [Router label and QR Code 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



Figure 1. Package contents

Your package contains following:

- NETGEAR Nighthawk AC2300 Cybersecurity WiFi Router
- Three Antennas
- Power adapter (varies by region)
- Yellow Ethernet cable
- Quick start guide

Attach the antennas

The router comes with three antennas.

To attach the antennas:

1. Remove the antenna caps from the antenna posts on the router.
2. Align the antennas with the antenna posts on the router.
3. Attach the antennas on the threaded antenna posts.



4. Position the antennas for the best WiFi performance.



We recommend that the center antenna be vertical and that you aim the others outward at 45-degree angles, as shown.

LEDs and buttons on the top panel

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

Table 1. LED and button descriptions







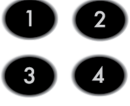


LEDs and Buttons	Descriptions
Power 	Solid amber. The router is starting. Blinking amber. The firmware is upgrading, or the Reset button was pressed. Solid white. The router is ready. Blinking white. The firmware is corrupted. Off. Power is not supplied to the router.
Internet 	Solid white. The Internet connection is ready. Solid amber. The router detected an Ethernet cable connection to the modem. Blinking white. The port is sending or receiving traffic. Off. No Ethernet cable is connected between the router and the modem.
2.4 GHz WiFi 	Solid white. The 2.4 GHz WiFi radio is operating. Blinking white. The router is sending or receiving WiFi traffic. Off. The 2.4 GHz WiFi radio is off.
5 GHz WiFi 	Solid white. The 5 GHz WiFi radio is operating. Blinking white. The router is sending or receiving WiFi traffic. Off. The 5 GHz WiFi radio is off.
USB 3.0 (front panel) 	Solid white. A USB storage device is connected and is ready. Blinking white. A USB storage device is plugged in and is trying to connect. Off. No USB storage device is connected, or someone clicked the Safely Remove Hardware button and it is now safe to remove the attached USB storage device.
USB 2.0 (rear panel) 	Solid white. A USB device is connected and is ready. Blinking white. A USB device is plugged in and is trying to connect. Off. No USB device is connected, or someone clicked the Safely Remove Hardware button and it is now safe to remove the attached USB device.

Table 1. LED and button descriptions (Continued)

LEDs and Buttons	Descriptions
LAN ports 1-4 	The LED color indicates the speed: white for Gigabit Ethernet connections and amber for 100 Mbps or 10 Mbps Ethernet connections. Solid white or solid amber. A powered-on device is connected to the Ethernet port. Blinking white or blinking amber. The port is sending or receiving traffic. Off. No device is connected to this Ethernet port.
WiFi On/Off button with LED 	Pressing this button for two seconds turns the 2.4 GHz and 5 GHz WiFi radios on and off. If this LED is solid white, the WiFi radios are on. If this LED is off, the WiFi radios are turned off and you cannot use WiFi to connect to the router.
WPS button with LED 	This button lets you use WPS to join the WiFi network without typing the WiFi password. The WPS LED blinks white during this process and then lights solid white.

Rear panel

The following figure shows the rear panel connectors and buttons.



Figure 2. Router rear panel

Nighthawk AC2300 Cybersecurity WiFi Router Model RS400

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

- **Reset button.** Pressing the **Reset** button resets the router. If you press the **Reset** button for at least 10 seconds, the Power LED blinks amber and the router returns to its factory settings.
- **LAN ports.** Four Gigabit Ethernet RJ-45 LAN ports to connect the router to LAN devices.
- **Internet port.** One Gigabit Ethernet RJ-45 WAN port to connect the router to an Internet modem such as a cable modem or DSL modem.
- **USB 2.0 port.** One USB 2.0 port to connect the router to a USB storage device that does not require a USB 3.0 connection.

Note: The USB 3.0 port is on the front panel. You can use the USB 3.0 port to connect the router to a USB storage device.

- **Power On/Off button.** Press the **Power On/Off** button to provide power to the router.
- **DC power connector.** Connect the power adapter that came with your router to the DC power connector.

Router label and QR Code label

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

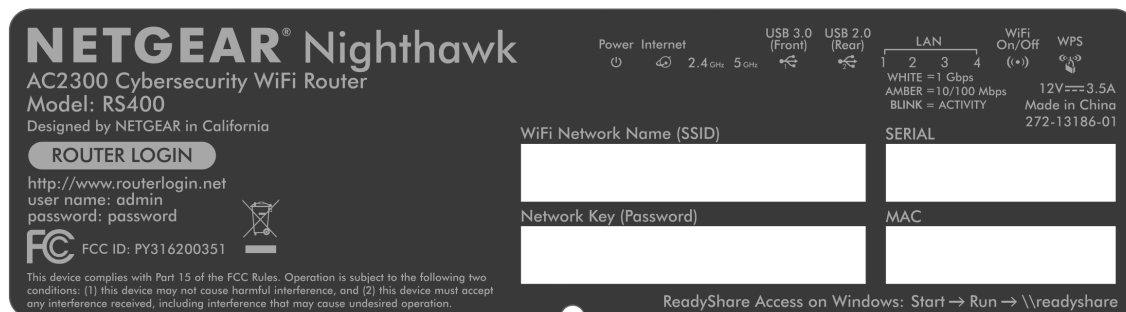


Figure 3. Router label

The QR code label is on the top panel.



Figure 4. QR code label location

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 computers.
- Place the router in an elevated location, minimizing the number walls and ceilings between the router and your other devices.
- Place the router away from electrical devices such as these:
 - Ceiling fans
 - Home security systems
 - Microwaves
 - Computers
 - Base of a cordless phone
 - 2.4 GHz or 5 GHz cordless phones

Nighthawk AC2300 Cybersecurity WiFi Router Model RS400

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

The following factors might limit the range of your WiFi:

- The thickness and number of walls the WiFi signal passes through 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

The following figure shows how to can cable your router.

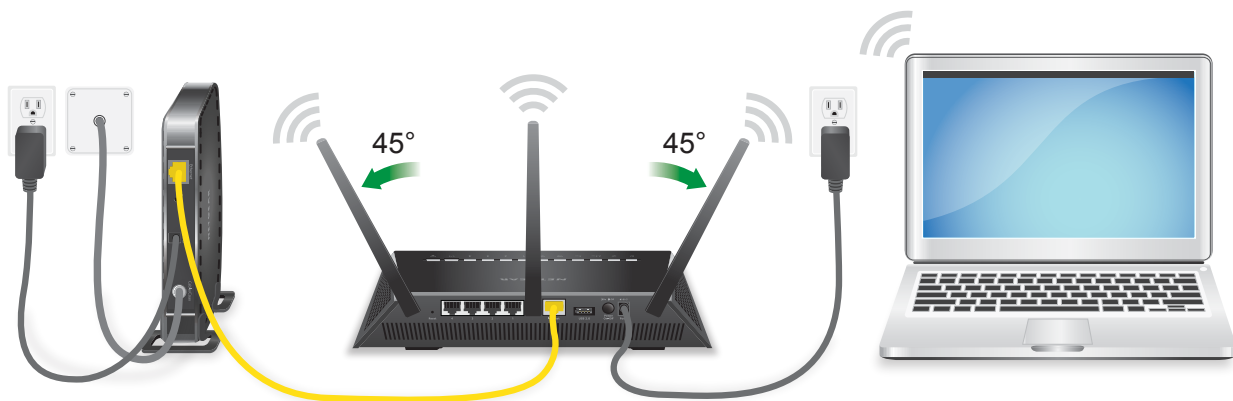


Figure 5. Cable your router

To cable your router:

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

2

Connect to the Router's Network and Automatically Set Up the Internet Connection

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

The chapter contains the following sections:

- [Connect to the network](#)
- [Types of logins](#)
- [Use a web browser to access the router](#)
- [Change the language](#)
- [Install and manage your router with the Nighthawk app](#)

Connect to the network

You can connect to the router's network through a wired or WiFi connection. If you set up your computer to use a static IP address, change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Connect to the network using a wired connection

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

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

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

Find and connect to the WiFi network

Note: If you use a smartphone or tablet, you can scan the QR code on the router to join its WiFi network. You can also use the following procedure.

To find and connect to the WiFi network:

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

WiFi connection using WPS

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

To use WPS to connect to the WiFi network:

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

Types of logins

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

Several types of logins are associated with the router:

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

Note: If your router is connected to the Internet, use the NETGEAR account email address and password to log in to the router. If your router is *not* connected to the Internet, use the admin user name and router login password to log in to the router.

Use a web browser to access the router

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

the router, the software automatically checks to see if your router can connect to your Internet service.

Use a web browser to set up the router's Internet connection automatically

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

When your Internet service starts, your Internet service provider (ISP) typically gives you all the information needed to connect to the Internet. For 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. 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 use a web browser to set up your router's Internet connection automatically:

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: When the router connects to the Internet, you are prompted to customize the router's WiFi network name and WiFi password. If you want to do so, use a wired connection to avoid being disconnected when the new WiFi settings take effect. You can also change the WiFi network name and WiFi password later.

3. Launch a web browser.

Your browser might display a security warning and might not let you proceed. You can either ignore this warning or add a security certificate as described in the following examples.

Note: For detailed information about security warnings and adding security certificates, see [Resolve a browser security warning](#) on page 170.

- If Google Chrome displays a *Your connection is not private* message or a similar warning, click the **ADVANCED** link. Then, click the **Proceed to 192.168.1.1 (unsafe)** link and install a security certificate.
- If Apple Safari displays a *This connection is not private* message or a similar warning, click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window opens, click the **Visit Website** button. If another pop-up window opens to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
- If Mozilla Firefox displays a *Your connection is not secure* message or a similar warning, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that opens, click the **Confirm Security Exception** button and install a security certificate.
- If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message or a similar warning, click the **Continue to this website (not recommended)** link and install a security certificate.
- If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage** and install a security certificate.

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 **<https://www.routerlogin.net>** and the Configuring the Internet Connection page displays.
- If you already set up the Internet connection, enter **<https://www.routerlogin.net>** in the address field for your browser to start the installation process.

4. Follow the onscreen instructions.

The router connects to the Internet.

5. If you already ignored the security warning or installed a security certificate but the browser still does not display the NETGEAR installation assistant, do the following:

- Make sure that the computer is connected to one of the LAN Ethernet ports or over WiFi to the router.
- Make sure that the router is receiving power and that its Power LED is lit.
- Close and reopen the browser or clear the browser cache.

- Browse to **<https://www.routerlogin.net>**.
 - If the computer is set to a static or fixed IP address (this setting is uncommon), change it to obtain an IP address automatically from the router.
6. If the router does not connect to the Internet, do the following:
- a. Review your settings. Make sure that you selected the correct options and typed everything correctly.
 - b. Contact your ISP to verify that you are using the correct configuration information.
 - c. Read [You cannot access the Internet](#) on page 175.
 - d. If problems persist, register your NETGEAR product and contact NETGEAR Technical Support.
- During the initial installation with the NETGEAR installation assistant, you are prompted to register your product.

When the router connects to the Internet, you are prompted to do the following:

- Change the password for the router admin user name and set up security questions.
- Customize your WiFi network name and password.
- Let the router check if a new firmware version is available and upgrade the firmware.
- Log in to NETGEAR Armor and activate your subscription.
- Register your product.
- Download the Nighthawk app.

Log in to the router

When you first connect to your router and launch a web browser, the browser automatically displays the router web interface. If you want to view or change settings for the router later, you can use a browser to log in to the router web interface.

Your browser might display a security warning and might not let you proceed. You can either ignore this warning or add a security certificate as described in the following examples.

Note: For detailed information about security warnings and adding security certificates, see [Resolve a browser security warning](#) on page 170.

- If Google Chrome displays a *Your connection is not private* message or a similar warning, click the **ADVANCED** link. Then, click the **Proceed to 192.168.1.1 (unsafe)** link and install a security certificate.

- If Apple Safari displays a *This connection is not private* message or a similar warning, click the **Show Details** button. Then, click the **visit this website** link. If a warning pop-up window opens, click the **Visit Website** button. If another pop-up window opens to let you confirm changes to your certificate trust settings, enter your Mac user name and password and click the **Update Setting** button.
- If Mozilla Firefox displays a *Your connection is not secure* message or a similar warning, click the **ADVANCED** button. Then, click the **Add Exception** button. In the pop-up window that opens, click the **Confirm Security Exception** button and install a security certificate.
- If Microsoft Internet Explorer displays a *There is a problem with this website's security certificate* message or a similar warning, click the **Continue to this website (not recommended)** link and install a security certificate.
- If Microsoft Edge displays a *There is a problem with this website's security certificate* message or a similar warning, select **Details > Go on to the webpage** and install a security certificate.

To log in to the router:

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

Note: You can also enter **http://www.routerlogin.com**, **https://192.168.1.1**, or **http://192.168.1.1**. If you enter one of these links starting with **http://**, the browser automatically redirects your request to **https://** (secure HTTP). The procedures in this manual use **http://www.routerlogin.net**.

Your browser might display a security message, which you can ignore (see the introduction to this task).

A login window opens.

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

Change the language

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

To change the language:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. In the upper right corner, select a language from the menu.
5. When prompted, click the **OK** button to confirm this change.
The page refreshes with the language that you selected.

Install and manage your router with the Nighthawk app

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

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

To install your router using the Nighthawk app:

1. To download the app, visit <https://www.netgear.com/home/apps-services/nighthawk-app/>.
2. On your mobile device, tap **Settings > Wi-Fi** and find and connect to your router's WiFi network.
Your router's WiFi network name (SSID) and network key (WiFi password) are on the router label.
If the label includes a QR code, you can scan the QR code to join the router's WiFi network.
3. Launch the Nighthawk app on your mobile device.
4. Follow the prompts on the app to install your router and connect to the Internet.

3

Specify Your Internet Settings

Usually, the quickest way to set up the router to use your Internet connection is to allow your router to detect the Internet connection automatically when you first access the router web interface. You can also customize and manually specify your Internet settings.

This chapter contains the following sections:

- [Use the Internet Setup Wizard](#)
- [Manually set up the Internet connection](#)
- [Specify IPv6 Internet connections](#)
- [Manage the MTU size](#)

Use the Internet Setup Wizard

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

To use the Setup Wizard:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Setup Wizard**.
The Setup Wizard page displays.
5. Select the **Yes** radio button.
If you select the **No** radio button, you are taken to the Internet Setup page (see [Manually set up the Internet connection](#) on page 26).
6. Click the **Next** button.
The Setup Wizard searches your Internet connection for servers and protocols to determine your Internet configuration.

Manually set up the Internet connection

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

Specify an Internet connection without a login

To specify the Internet connection settings:

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

3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Internet**.
The Internet Setup page displays.
5. In the Does your Internet connection require a login? section, leave the **No** radio button selected.
6. If your Internet connection requires an account name or host name, click the **Edit** button in the Account Name section and enter the account name.
7. If your Internet connection requires a domain name, type it in the **Domain Name (If Required)** field.
For the other sections on this page, the default settings usually work, but you can change them.
8. Select an Internet IP Address radio button:
 - **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
 - **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP router to which your router connects.
9. Select a Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
 - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
10. Select a Router MAC Address radio button:
 - **Use Default Address**. Use the default MAC address.
 - **Use Computer MAC Address**. The router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
 - **Use This MAC Address**. Enter the MAC address that you want to use.
11. Click the **Apply** button.
Your settings are saved.

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

If the NETGEAR website does not display within one minute, see [You cannot access the Internet](#) on page 175.

Specify an Internet connection that uses a login and PPPoE service

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

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Internet**.
The Internet Setup page displays.
5. Select the Does your Internet connection require a login? **Yes** radio button.
The page adjusts.
6. From the **Internet Service Provider** menu, select **PPPoE** as the encapsulation method.
The page adjusts.
7. In the **Login** field, enter the login name that your ISP gave you.
This login name is often an email address.
8. In the **Password** field, type the password that you use to log in to your Internet service.
9. If your ISP requires a service name, type it in the **Service Name (if Required)** field.

10. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.
11. To change the number of minutes until the Internet login times out, in the **Idle Timeout (In minutes)** field, type the number of minutes.
This is how long the router keeps the Internet connection active when no one on the network is using the Internet connection. A value of 0 (zero) means never log out.
12. Select an Internet IP Address radio button:
 - **Get Dynamically from ISP.** Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
 - **Use Static IP Address.** Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP router to which your router connects.
13. Select a Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
 - **Use These DNS Servers.** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
14. Select a Router MAC Address radio button:
 - **Use Default Address.** Use the default MAC address.
 - **Use Computer MAC Address.** The router captures and uses the MAC address of the computer that you are now using. You must use the one computer that the ISP allows.
 - **Use This MAC Address.** Enter the MAC address that you want to use.
15. Click the **Apply** button.
Your settings are saved.
16. Click the **Test** button to test your Internet connection.
If the NETGEAR website does not display within one minute, see [You cannot access the Internet](#) on page 175.

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

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

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

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Internet**.
The Internet Setup page displays.
5. Select the Does your Internet connection require a login? **Yes** radio button.
The page adjusts.
6. From the **Internet Service Provider** menu, select **PPTP** or **L2TP** as the encapsulation method.
The page adjusts.
7. In the **Login** field, enter the login name that your ISP gave you.
This login name is often an email address.
8. In the **Password** field, type the password that you use to log in to your Internet service.
9. From the **Connection Mode** menu, select **Always On**, **Dial on Demand**, or **Manually Connect**.
10. To change the number of minutes until the Internet login times out, in the **Idle Timeout (In minutes)** field, type the number of minutes.
This is how long the router keeps the Internet connection active when no one on the network is using the Internet connection. A value of 0 (zero) means never log out.
11. If your ISP gave you fixed IP addresses and a connection ID or name, type them in the **My IP Address**, **Subnet Mask**, **Server Address**, **Gateway IP Address**, and **Connection ID/Name** fields.
If your ISP did not give you IP addresses, a connection ID, or name, leave these fields blank. The connection ID or name applies to a PPTP service only.

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

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

13. Select a Router MAC Address radio button:

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

14. Click the **Apply** button.

Your settings are saved.

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

If the NETGEAR website does not display within one minute, see [You cannot access the Internet](#) on page 175.

Specify IPv6 Internet connections

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

To set up an IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select the IPv6 connection type:
 - If you are not sure, select **Auto Detect** so that the router detects the IPv6 type that is in use.

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

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

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

Requirements for entering IPv6 addresses

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

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

Use Auto Detect for an IPv6 Internet connection

To set up an IPv6 Internet connection through autodetection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Detect**.
The page adjusts.
The router automatically detects the information in the following fields:
 - **Connection Type**. This field indicates the connection type that is detected.
 - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the

length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.

- **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.

6. Select an IP Address Assignment radio button:

- **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCv6 client function.
- **Auto Config.** This is the default setting.

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

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

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

8. Click the **Apply** button.

Your settings are saved.

Set up an IPv6 6to4 tunnel Internet connection

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

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

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

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

A login window opens.

3. Enter the router admin user name and password.

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

The BASIC Home page displays.

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

The IPv6 page displays.

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

The page adjusts.

The router automatically detects the information in the Router's IPv6 Address on LAN field. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.

6. Select a Remote 6to4 Relay Router radio button:

- **Auto.** Your router uses any remote relay router that is available on the Internet. This is the default setting.
- **Static IP Address.** Enter the static IPv4 address of the remote relay router. Your IPv6 ISP usually provides this address.

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

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

8. Select an IP Address Assignment radio button:

- **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCPv6 client function.
- **Auto Config.** This is the default setting.

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

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

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

10. Click the **Apply** button.

Your settings are saved.

Set up an IPv6 pass-through Internet connection

In pass-through mode, the router works as a Layer 2 Ethernet switch with two ports (LAN and WAN Ethernet ports) for IPv6 packets. The router does not process any IPv6 header packets.

To set up a pass-through IPv6 Internet connection:

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

Set up a fixed IPv6 Internet connection

To set up a fixed IPv6 Internet connection:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
The IPv6 page displays.

5. From the **Internet Connection Type** menu, select **Fixed**.
The page adjusts.
6. Configure the fixed IPv6 addresses for the WAN connection:
 - **IPv6 Address/Prefix Length.** The IPv6 address and prefix length of the router WAN interface.
 - **Default IPv6 Gateway.** The IPv6 address of the default IPv6 gateway for the router's WAN interface.
 - **Primary DNS Server.** The primary DNS server that resolves IPv6 domain name records for the router.
 - **Secondary DNS Server.** The secondary DNS server that resolves IPv6 domain name records for the router.

Note: If you do not specify the DNS servers, the router uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup page. (See [Manually set up the Internet connection](#) on page 26.)

7. Select an IP Address Assignment radio button:
 - **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCv6 client function.
 - **Auto Config.** This is the default setting.

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

8. In the **IPv6 Address/Prefix Length** fields, specify the static IPv6 address and prefix length of the router's LAN interface.
If you do not specify an ID here, the router generates one automatically from its MAC address.

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

Set up an IPv6 DHCP Internet connection

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

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

3. Enter the router admin user name and password.

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

The BASIC Home page displays.

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

The IPv6 page displays.

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

The page adjusts.

The router automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.

6. (Optional) In the **DHCP User Class (If Required)** field, enter a host name.

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

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

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

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

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

9. Select an IP Address Assignment radio button:

- **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCv6 client function.
- **Auto Config.** This is the default setting.

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

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

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

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

Set up an IPv6 PPPoE Internet connection

To set up a PPPoE IPv6 Internet connection:

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

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

A login window opens.

3. Enter the router admin user name and password.

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

The BASIC Home page displays.

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

The IPv6 page displays.

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

The page adjusts.

The router automatically detects the information in the following fields:

- **Router's IPv6 Address on WAN.** This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (__) under the IPv6 address. If no address is acquired, the field displays Not Available.
- **Router's IPv6 Address on LAN.** This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the

prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.

6. In the **Login** field, enter the login information for the ISP connection.
This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, you would type JerAB in this field. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.
7. In the **Password** field, enter the password for the ISP connection.
8. In the **Service Name** field, enter a service name.
If your ISP did not provide a service name, leave this field blank.

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

9. Select an IPv6 Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
 - **Use These DNS Servers.** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
10. Select an IP Address Assignment radio button:
 - **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCv6 client function.
 - **Auto Config.** This is the default setting.

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

11. (Optional) Select the **Use This Interface ID** check box and specify the interface ID to be used for the IPv6 address of the router's LAN interface.
If you do not specify an ID here, the router generates one automatically from its MAC address.
12. Click the **Apply** button.
Your settings are saved.

Use Auto Config for an IPv6 Internet connection

To set up an IPv6 Internet connection through autoconfiguration:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > IPv6**.
The IPv6 page displays.
5. From the **Internet Connection Type** menu, select **Auto Config**.
The page adjusts.
The router automatically detects the information in the following fields:
 - **Router's IPv6 Address on WAN**. This field shows the IPv6 address that is acquired for the router's WAN (or Internet) interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
 - **Router's IPv6 Address on LAN**. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline () under the IPv6 address. If no address is acquired, the field displays Not Available.
6. (Optional) In the **DHCP User Class (If Required)** field, enter a host name.
Most people can leave this field blank, but if your ISP gave you a specific host name, enter it here.
7. (Optional) In the **DHCP Domain Name (If Required)** field, enter a domain name.
You can type the domain name of your IPv6 ISP. Do not enter the domain name for the IPv4 ISP here. For example, if your ISP's mail server is mail.xxx.yyy.zzz, type xxx.yyy.zzz as the domain name. If your ISP provided a domain name, type it in this field. For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.

8. Select an IPv6 Domain Name Server (DNS) Address radio button:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
 - **Use These DNS Servers.** If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
9. Select an IP Address Assignment radio button:
 - **Use DHCP Server.** This method passes more information to LAN devices but some IPv6 systems might not support the DHCv6 client function.
 - **Auto Config.** This is the default setting.

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

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

Your settings are saved.

Set up an IPv6 6rd tunnel connection

The 6rd protocol makes it possible to deploy IPv6 to sites using a service provider's IPv4 network. 6rd uses the service provider's own IPv6 address prefix. This limits the operational domain of 6rd to the service provider's network and is under direct control of the service provider. The IPv6 service that is provided is equivalent to native IPv6.

The 6rd mechanism relies on an algorithmic mapping between the IPv6 and IPv4 addresses that are assigned for use within the service provider's network. This mapping allows for automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, enabling stateless operation of 6rd.

To set up an IPv6 6rd tunnel connection:

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

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

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

The BASIC Home page displays.

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

The IPv6 page displays.

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

The page adjusts.

The router automatically detects the information in the Router's IPv6 Address on LAN field. This field shows the IPv6 address that is acquired for the router's LAN interface. The number after the slash (/) is the length of the prefix, which is also indicated by the underline (_) under the IPv6 address. If no address is acquired, the field displays Not Available.

6. In the 6rd Configuration section, configure the 6rd settings:

- **6rd Prefix**. Enter the IPv6 prefix that your ISP gave you.
- **6rd Prefix Length**. Enter the IPv6 prefix length that your ISP gave you.
- **6rd Border Relay Address**. Enter the border router's IPv4 address that your ISP gave you.
- **6rd Address Mask Length**. Enter the IPv4 mask length that your ISP gave you.

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

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

8. Select an IP Address Assignment radio button:

- **Use DHCP Server**. This method passes more information to LAN devices but some IPv6 systems might not support the DHCv6 client function.
- **Auto Config**. This is the default setting.

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

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

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

10. (Optional) Change the MTU size in bytes by specifying a new size in the field.
The default size 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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Setup > WAN Setup**.
The WAN Setup page displays.
5. In the **MTU Size** field, enter a value from 64 to 1500.
6. Click the **Apply** button.
Your settings are saved.

4

Control Access to the Internet

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

This chapter includes the following sections:

- [Manage NETGEAR Armor](#)
- [Enable Circle with Disney](#)
- [Enable access control to allow or block access to the Internet](#)
- [Manage network access control lists](#)
- [Use keywords to block Internet sites](#)
- [Delete keywords from the blocked list](#)
- [Prevent blocking on a trusted computer](#)
- [Block services from the Internet](#)
- [Schedule when to block Internet sites and services](#)
- [Set up security event email notifications](#)

Manage NETGEAR Armor

In addition to built-in security features, your router includes a 3-year subscription to NETGEAR Armor.

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

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

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

We recommend that you manage NETGEAR Armor from the Nighthawk app. However you can use the router web interface to sign in to NETGEAR Armor and start your subscription. After you activate NETGEAR Armor, you can temporarily disable it. You can also reenable it again.

To view or change your Armor settings, use the NETGEAR Armor portal.

Activate Armor using the Nighthawk app

To activate Armor using the Nighthawk app:

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

View or change your NETGEAR Armor settings using the Nighthawk app

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

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

The Armor page displays.

You can now view or change the settings.

View or change your NETGEAR Armor settings from the Armor portal

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

To view or change your NETGEAR Armor settings:

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

Sign in to NETGEAR Armor from the router web interface and start your subscription

Your router includes a NETGEAR Armor subscription. If you did not activate NETGEAR Armor during the router installation process, you can use the router web interface to activate NETGEAR Armor and start your subscription.

To sign in to NETGEAR Armor from the router web interface and start your subscription:

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

6. Enter your NETGEAR account email address and password in the fields and then click the **LOGIN** button.

If you did not create a NETGEAR account, visit netgear.com/mynetgear and register your router to create a NETGEAR account.

The router contacts the NETGEAR server and NETGEAR Armor is activated.

Access the NETGEAR Armor portal from the router web interface

If you already activated NETGEAR Armor, you can access the NETGEAR Armor portal through the router web interface.

To view or change your NETGEAR Armor settings from the router web interface:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Scroll down to the NETGEAR Armor pane and click the **Launch NETGEAR Armor** button.
The NETGEAR account sign in page displays.
5. Enter your NETGEAR account email address and password in the fields and then click the **Sign In** button.
The NETGEAR Armor portal displays.

Disable or Reenable NETGEAR Armor from the router web interface

If you already activated NETGEAR Armor, you can temporarily disable it. You can also reenable it again.

To disable or reenable NETGEAR Armor from the router web interface:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **NETGEAR Armor**.
The NETGEAR Armor Protection page displays.
5. Set the NETGEAR Armor Status button to **Enabled** or to **Disabled**.
6. Click the **Apply** button.
You settings are saved.
If NETGEAR Armor is enabled, the Status field displays Protected.
If NETGEAR Armor is disabled, the Status field displays Not protected.

Enable Circle with Disney

Circle with Disney is a parental control technology that helps you monitor your children's devices that are connected to your network.

You can enable Circle using your router web interface or you can enable Circle using the Circle app.

After you enable Circle, you can do the following with the Circle app:

- Set time limits for daily Internet usage
- Set individual filter levels for each family member
- Set a bedtime for your family member's devices
- Pause the Internet
- Manage your family's mobile devices across all networks with Circle Go

For more information about Circle with Disney, visit www.netgear.com/circle.

Enable Circle with Disney using the Nighthawk app

Before enabling Circle, make sure that your router is in router mode (which is the default mode). Your router must be in router mode to work with Circle. You can't enable Circle if your router is in access point (AP) mode or bridge mode.

To enable Circle with Disney using the Nighthawk app:

1. Launch the Nighthawk app.
The dashboard displays.
2. Tap **Parental Controls**.
The Parental Control page displays.
3. Move the **Enable Circle** slider to the right to enable Circle with Disney.
4. Tap the **Download and Install Circle App** button.
5. Download the Circle app.
You must use the Circle app to finish setting up your Circle account.
6. Launch the Circle app and follow the prompts.

Enable Circle with Disney using the Circle app

Before enabling Circle, make sure that your router is in router mode (which is the default mode). Your router must be in router mode to work with Circle. You can't enable Circle if your router is in access point (AP) mode or bridge mode.

If your router is not running the latest firmware, the Circle app checks your router's firmware and updates the firmware for you.

To enable Circle with Disney using the Circle app:

1. Make sure that your mobile device is connected to your router's network.
2. Download the Circle app on your mobile device.
3. Launch the Circle app.
4. Follow the prompts to set up Circle.

Enable access control to allow or block access to the Internet

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

To set up access control:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Security > Access Control**.
The Access Control page displays.
5. Select the **Turn on Access Control** check box.
You must select this check box before you can specify an access rule and use the **Allow** and **Block** buttons. When this check box is cleared, all devices are allowed to connect, even if a device is in the blocked list.
6. Select an access rule:
 - **Allow all new devices to connect.** With this setting, a new device can access your network. You don't need to enter the its MAC address. This is the default setting. We recommend that you leave this radio button selected.
 - **Block all new devices from connecting.** With this setting, a new device cannot access your router's Internet connection, but can still access your router's local network. Before a device accesses your router's Internet connection, you must enter its MAC address for an Ethernet connection and its MAC address for a WiFi connection in the allowed list.

The access rule does not affect previously blocked or allowed devices. It applies only to devices joining your network in the future after you apply these settings.
7. To view allowed or blocked devices that are not connected, click one of the following links:
 - **View list of allowed devices not currently connected to the network**
 - **View list of blocked devices not currently connected to the network**

The list displays.

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

Manage network access control lists

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

To manage devices that are allowed or blocked:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Security > Access Control**.
The Access Control page displays.
5. Select the **Turn on Access Control** radio button.
6. Click the **View list of allowed devices not currently connected to the network** link.
The list displays.
7. Select the check box for a device.
8. Use the **Add** button, **Edit** button, and **Remove from the list** button as needed.
9. Click the **Apply** button.
Your settings are saved.

Use keywords to block Internet sites

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

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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Sites**.
The Block Sites page displays.
5. Select a keyword blocking option:
 - **Per Schedule**. Turn on keyword blocking according to a schedule that you set. For more information, see [Schedule when to block Internet sites and services](#) on page 56.
 - **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>.
 - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
 - Enter a period (.) to block all Internet browsing access.
7. Click the **Add Keyword** button.
The keyword is added to the keyword list. The keyword list supports up to 32 entries.
8. Click the **Apply** button.
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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Security > 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 73.

To specify a trusted computer:

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

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

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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Security > Block Services**.
The Block Services page displays.
5. Specify when to block the services:
 - To block the services all the time, select the **Always** radio button.
 - To block the services based on a schedule, select the **Per Schedule** radio button.

For information about how to specify the schedule, see [Schedule when to block Internet sites and services](#) on page 56.

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, the same schedule is used to block sites and to block services.

To schedule blocking:

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

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

The BASIC Home page displays.

4. Select **ADVANCED > Security > Schedule**.

The Schedule page displays.

5. Specify when to block keywords and services:

- **Days to Block.** Select the check box for each day that you want to block the keywords, or select the **Every Day** check box, which automatically selects the check boxes for all days.
- **Time of Day to Block.** Select 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 opens.

3. Enter the router admin user name and password.

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

The BASIC Home page displays.

4. Select **ADVANCED > Security > E-mail**.

The E-mail page displays.

5. Select the **Turn E-mail Notification On** check box.

6. In the **Send to This E-mail Address** field, type the email address to which logs and alerts are to be sent.

This email address is also used for the From address. If this field is blank, log and alert messages are not sent.

7. In the **Sender** field, enter the email sender's name.
8. In the **Your Outgoing Mail Server** field, enter the name of your ISP outgoing (SMTP) mail server (such as mail.myISP.com).
You might be able to find this information in the configuration window of your email program. If you leave this field blank, log and alert messages are not sent.
9. In the **Outgoing Mail Server Port Number** field, enter a port number in the field. If you do not know the port number, leave the default port number.
10. 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.
11. 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.
12. To send logs based on a schedule, specify these settings:
 - a. From **Send logs according to this schedule** menu, select the schedule type.
 - b. From the **Day** menu, select the day.
 - c. From the **Time** menu, select the time, and select the **am** or **pm** radio button.
13. 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.

5

Optimize Performance

You can set up the router to optimize performance for applications such as Internet gaming, high-definition video streaming, and VoIP communication. By default, the router uses Wi-Fi Multimedia Quality of Service (WMM QoS).

This chapter contains the following sections:

- [Use Dynamic QoS to optimize Internet traffic management](#)
- [Wi-Fi Multimedia Quality of Service](#)
- [Improve network connections with Universal Plug and Play](#)
- [Enable or disable Smart Connect](#)

Use Dynamic QoS to optimize Internet traffic management

Dynamic 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. Dynamic QoS resolves traffic congestion when the Internet bandwidth is limited and different demands compete for bandwidth.

Enable Dynamic QoS

Because not everyone uses Dynamic QoS, it is disabled by default.

To enable Dynamic QoS:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Dynamic QoS**.
The Dynamic QoS page displays.
5. Select the **Enable Dynamic QoS** check box.
6. Specify your Internet bandwidth:
 - **Let Speedtest detect my Internet bandwidth**. We recommend that you use Speedtest to detect your Internet bandwidth.
To use Speedtest, do the following:
 - a. For more accurate Speedtest 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.
Speedtest determines your Internet bandwidth.

- **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.

Enable or disable the automatic QoS database update

The router uses a QoS database of the most popular applications and services to implement dynamic QoS. By default, the router automatically updates this database. If you enabled dynamic QoS, you can turn off this feature and manually update the database.

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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Dynamic QoS**.
The Dynamic QoS page displays.
5. Select or clear the **Automatically update performance optimization database** check box.
6. Click the **Apply** button.
Your settings are saved.

Manually update the Dynamic QoS database

The router uses a QoS database of the most popular applications and services to implement Dynamic QoS. By default, the router automatically updates this database when you enable Dynamic QoS, but if you turned off the automatic update feature, you can manually update the database.

To manually update the Dynamic QoS database:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Dynamic QoS**.
The Dynamic QoS page displays.
5. Click the **Update Now** button.
The router checks for the newest version of the database and downloads it.
6. Click the **Apply** button.
Your settings are saved.

Wi-Fi Multimedia Quality of Service

Wi-Fi Multimedia Quality of Service (WMM QoS) prioritizes WiFi voice and video traffic over the WiFi link. WMM QoS 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 WiFi 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 2.4 GHz or 5 GHz, the maximum link rate your router can reach is 54 Mbps.

To disable the WMM settings:

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

A login window opens.

3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Setup > QoS Setup**.
The Dynamic QoS page displays.
5. Click the **WMM** tab.
The page adjusts.
6. Clear the **Enable WMM (Wi-Fi multimedia) settings (2.4GHz b/g/n)** check box.
7. Clear the **Enable WMM (Wi-Fi multimedia) settings (5GHz a/n/ac)** check box.
8. Click the **Apply** button.
Your settings are saved.

Improve network connections with Universal Plug and Play

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

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance, enable UPnP.

To enable Universal Plug and Play:

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

The UPnP page displays.

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

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

6. Type the advertisement period in minutes.

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

7. Type the advertisement time to live in hops.

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

8. Click the **Apply** button.

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

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

Enable or disable Smart Connect

Smart Connect selects the fastest WiFi band for your device. For Smart Connect to work, the 2.4 GHz and 5 GHz bands must use the same WiFi network name (SSID) and network key (password). That means that when you connect to the router with WiFi, you see only one SSID that connects to both bands.

Note: If you enable Smart Connect and the SSID and passwords for the 2.4 GHz and 5 GHz bands do not match, the WiFi settings for 2.4 GHz band overwrites the WiFi settings for 5 GHz band.

To enable or disable Smart Connect:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Wireless**.
The Wireless Setup page displays.
5. Select or clear the **Enable Smart Connect** check box.
Selecting this check box turns on Smart Connect and clearing this check box turns off Smart Connect.
6. Click the **Apply** button.
Your settings are saved.

6

Manage Network Settings

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

This chapter includes the following sections:

- [View or change the WAN settings](#)
- [Set up a default DMZ server](#)
- [Change the LAN TCP/IP settings](#)
- [Change the router's device name](#)
- [Specify the IP addresses that the router assigns](#)
- [Disable the DHCP server feature in the router](#)
- [Manage reserved LAN IP addresses](#)
- [Set up the router as a WiFi access point](#)
- [Set up the router in bridge mode](#)
- [Return the router to router mode](#)
- [Set up a bridge for a port group or VLAN tag group](#)
- [Manage custom static routes](#)

View or change the WAN settings

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

To view or change the WAN settings:

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

View or change the following settings:

- **Disable Port Scan and DoS Protection.** DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, and many others. Select this check box only in special circumstances.
- **Default DMZ Server.** This feature is sometimes helpful when you are playing online games or videoconferencing, but it makes the firewall security less effective.
- **Respond to Ping on Internet Port.** This feature allows your router to be discovered. Use this feature only as a diagnostic tool or for a specific reason.
- **Disable IGMP Proxying.** IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. If you do not need this feature, you can select this check box to disable it.
- **MTU Size (in bytes).** The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. Change the MTU only if you are sure that it is necessary for your ISP connection.
- **NAT Filtering.** Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT protects computers on the LAN from attacks from the Internet but might prevent some Internet games, point-to-point applications, or multimedia applications from working. Open NAT provides a much less secured firewall but allows almost all Internet applications to work.

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

5. Click the **Apply** button.

Your settings are saved.

Set up a default DMZ server

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

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

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

To set up a default DMZ server:

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

5. Select the **Default DMZ Server** check box.
6. Type the IP address.
7. Click the **Apply** button.
Your settings are saved.

Change the LAN TCP/IP settings

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

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

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

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

To change the LAN TCP/IP settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
The LAN Setup page displays.
5. In the **IP Address** field, type the IP address.
6. In the **IP Subnet Mask** field, type the subnet mask of the router.
The IP address and subnet mask identify which addresses are local to a specific device and which must be reached through a gateway or router.
7. Change the RIP settings.

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

a. Select the RIP direction:

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

b. Select the RIP version:

- **Disabled.** This is the default setting.
- **RIP-1.** This format is universally supported. It is adequate for most networks, unless you are using an unusual network setup.
- **RIP-2.** This format carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

8. Click the **Apply** button.

Your settings are saved.

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

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

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 opens.

3. Enter the router admin user name and password.

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

The BASIC Home page displays.

4. Select **ADVANCED > Setup > Device Name**.

The Device Name page displays.

5. In the **Device Name** field, type a new name.
6. Click the **Apply** button.
Your settings are saved.

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The 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.
This IP address must be in the same subnet as the router.
 - b. In the **Ending IP Address** field, type the number at the end of the range of IP addresses.
This IP address must be in the same subnet as the router.
7. Click the **Apply** button.
Your settings are saved.

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

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

To disable the DHCP server feature in the router:

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

Manage reserved LAN IP addresses

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

Reserve 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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
The LAN Setup page displays.
5. In the Address Reservation section, click the **Add** button.
The Address Reservation page displays.

Tip: If the device for which you want to reserve an IP address is already on your network, you can select its associated radio button in the Address Reservation Table so that you don't have to manually enter the information that is described in the following three steps.

6. 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.

7. In the **MAC Address** field, type the MAC address of the device.
8. In the **Device Name** field, type a name for the device.
9. Click the **Apply** button.
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 contacts the router's DHCP server. Reboot the device, or access its IP configuration and force a DHCP release and renew.

Edit a reserved IP address

To edit a reserved address entry:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Setup > LAN Setup**.
The LAN Setup page displays.
5. Select the radio button next to the reserved address that you want to edit.
6. Click the **Edit** button.
The Address Reservation page displays.
7. Change the settings.
8. Click the **Apply** button.
Your settings are saved.

Delete a reserved IP address entry

To delete a reserved address entry:

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

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.

To set up the router as an AP:

1. Use an Ethernet cable to connect the Internet port of this router to an Ethernet port on the other router.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.
A login window opens.
4. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Router/ AP / Bridge Mode**.

The Router / AP / Bridge Mode page displays.

6. Select **AP Mode**.

The page adjusts.

7. Select an IP address setting:

- **Get dynamically from existing router.** The other router on the network assigns an IP address to this router while it is in AP mode.
- **Use fixed IP settings on this device (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.

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

8. Click the **Apply** button.

The IP address of the router changes, and you are disconnected.

9. To reconnect, close and restart your browser and type **<http://www.routerlogin.net>**.

Set up the router in bridge mode

You can use your router in bridge mode to connect multiple devices wirelessly at the faster 802.11ac speed. You need two routers: one set up as a router and the other set up as a bridge.

Installing your router as a bridge offers the following benefits:

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

For example, you can install the first router in a room like a home office where your Internet connection is located, then set up the second router in bridge mode. Place the router in bridge mode in a different room with your home entertainment center. Cable the router in bridge mode to your Smart TV, DVR, game console or Blu-ray player, and use its 802.11ac WiFi connection to the first router.

To set up the router in bridge mode:

1. Make a note of the WiFi settings of the other router to which this router will connect. You must know the SSID, WiFi security mode, wireless password, and operating frequency (either 2.4 GHz or 5 GHz).
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.
A login window opens.
4. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Router/ AP / Bridge Mode**.
The Router / AP / Bridge Mode page displays.
6. Select **Bridge Mode**.
The page adjusts.
7. Click the **setup bridge mode wireless settings** button.
The Wireless Settings window opens.
8. Specify the settings of the other router to which this router will connect:
 - a. Select the wireless network frequency (**2.4 GHz** or **5 GHz**).
For 802.11ac mode, select **5 GHz**.
 - b. In the **Name (SSID)** file, enter the wireless network name (SSID).
 - c. In the Security Options section, select a radio button.
 - d. If prompted, type the WiFi password (network key) that you use to connect wirelessly to the other router.
9. Click the **Apply** button.
The settings for the other router are saved and the Router / AP / Bridge Mode page displays.
10. Click the **Apply** button on the Router / AP / Bridge Mode page.
Your settings are saved.

Return the router to router mode

By default, your router is set to router mode. If you changed the mode to access point mode or bridge mode, you can change the mode back to router mode.

To set up 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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Router/ AP / Bridge Mode**.
The Router / AP / Bridge Mode page displays.
5. Select **Router Mode**.
The page adjusts.
6. Click the **Apply** button.
Your settings are saved.

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

Some devices, such as an IPTV, cannot function behind the router's network address translation (NAT) service or firewall. Based on what your Internet service provider (ISP) requires, for the device to connect to the ISP's network directly, you can enable the bridge between the device and the router's Internet port or add new VLAN tag groups to the bridge.

Note: If your ISP provides instructions 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 a port group for the router's Internet interface.

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

To configure a port group and enable the bridge:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
 2. Enter **http://www.routerlogin.net**.
A login window opens.
 3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
 4. Select **ADVANCED > Advanced Setup > VLAN / Bridge Settings**.
The VLAN / Bridge Settings page displays.
 5. Select the **Enable VLAN / Bridge Setup** check box.
The page expands.
 6. Select the **By bridge group** radio button.
The page expands.
 7. Select a Wired Ports check box or a Wireless check box:
 - If your device is connected to an Ethernet port on the router, select the Wired Ports check box that corresponds to the Ethernet port on the router to which the device is connected.
 - If your device is connected to your router's WiFi network, select the Wireless check box that corresponds to the router's WiFi network to which the device is connected.
- Note:** You must select at least one Wired Ports or Wireless check box. You can select more than one check box.
8. Click the **Apply** button.
Your settings are saved.

Set up a bridge for a VLAN tag group

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

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

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

To add a VLAN tag group and enable the bridge:

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

9. Select the check box for a wired LAN port or WiFi port.

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

You must select at least one LAN port or WiFi port. You can select more than one port.

10. Click the **Add** button.

The VLAN tag group is added.

11. Click the **Apply** button.

Your settings are saved.

Manage custom static routes

Typically, you do not need to add static routes unless you use multiple routers or multiple IP subnets on your network.

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

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

When you set up your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you try to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the company firewall is likely to deny the request.

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

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** field specifies that all traffic for these addresses will be forwarded to the ISDN router at 192.168.1.100.

- A metric value of 1 works because the ISDN router is on the LAN.
- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

Set up a static route

To set up a static route:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.
The Static Routes page displays.
5. Click the **Add** button.
The page adjusts.
6. 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.
The IP address of the gateway must be on the same LAN segment as the router.
 - **Metric.** Enter a number from 1 through 15.

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

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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Static Routes**.
The Static Routes page displays.
5. In the table, select the radio button for the route.
6. Click the **Edit** button.
The Static Routes page adjusts.
7. Edit the route information.
8. Click the **Apply** button.
Your settings are saved.

Delete a static route

To delete a static route:

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

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

7

Manage the WiFi Network Settings

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

The chapter includes the following sections:

- [Use the WPS Wizard for WiFi connections](#)
- [Specify basic WiFi settings](#)
- [Change the WiFi password or the WiFi security](#)
- [Set up WPA/WPA2 enterprise WiFi security](#)
- [Set up WEP legacy WiFi security](#)
- [Change the WiFi Mbps settings](#)
- [Change the transmission power of the WiFi radios](#)
- [Set up a guest WiFi network](#)
- [Control the WiFi radios](#)
- [Set up a WiFi schedule](#)
- [Manage WPS settings](#)
- [Enable or disable implicit beamforming](#)
- [Enable or disable airtime fairness](#)
- [Enable or disable MU-MIMO](#)
- [Manage advanced WiFi settings](#)

Use the WPS Wizard for WiFi connections

The WPS Wizard helps you add a WPS-enabled device to your WiFi network without typing the WiFi password.

To use the WPS Wizard:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > WPS Wizard**.
A note explaining WPS displays.
5. Click the **Next** button.
The WPS page displays.
6. Select a setup method:
 - **Push button**. Click the **WPS** button on this page.
 - **PIN Number**. The page adjusts. Enter the client security PIN and click the **Next** button.
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 your WPS-enabled device with the network password when it connects. The router WPS page displays a confirmation message.

Specify basic WiFi settings

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

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

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

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

To specify basic WiFi settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Wireless**.
The Wireless Setup page displays.
You can specify the settings for the 2.4 GHz band and 5 GHz band.
5. From the **Region** menu, select your region.
In some locations, you cannot change this setting.
6. To control the SSID broadcast, select or clear the **Enable SSID Broadcast** check box.
When this check box is selected, the router broadcasts its network name (SSID) so that it displays when you scan for local WiFi networks on your computer or WiFi device.
7. Select or clear the **Enable 20/40 MHz Coexistence check box**.
Disabling this option allows your 2.4 GHz WiFi to keep its maximum speed. Enabling this option might reduce the maximum speed of your 2.4 GHz WiFi to the half if another WiFi network is detected in your environment; this is to avoid interference between WiFi networks and to get along with other WiFi networks in the environment.
8. To change the network name (SSID), type a new name in the **Name (SSID)** field.
The name can be up to 32 characters long and it is case-sensitive. The default SSID is randomly generated and is on the router label. If you change the name, make sure to write down the new name and keep it in a safe place.
9. To change the WiFi channel, select a number from the **Channel** menu.

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

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

10. Click the **Apply** button.

Your settings are saved.

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

11. Make sure that you can reconnect over WiFi to the network with its new settings.

If you cannot connect over WiFi, check the following:

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

Change the WiFi password or the WiFi security

The WiFi password is the one that you use to connect to the router's WiFi network so that you can access the Internet and other shared network resources.

Your router comes with preset WPA2-PSK security. We recommend that you use the preset security. The preset WiFi password is on the router label, but you can customize the WiFi password for greater security.

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

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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Wireless**.
The Wireless Setup page displays.
5. To change the 2.4 GHz or 5 GHz WiFi password, enter a new password in the **Password (Network Key)** field.
You must enter a phrase of 8 to 63 characters. The **Password (Network Key)** field displays if you select the **WPA2-PSK [AES]** or **WPA-PSK [TKIP] + WPA2-PSK [AES]** security radio button.
6. To change the WiFi security for the 2.4 GHz or 5 GHz WiFi network, select a Security Options radio button.
 - **WPA2-PSK [AES]**. This option is the default setting. This type of security enables WiFi devices that support WPA2 to join the router's WiFi network. If you did not change the WiFi password, the default password displays. The default password is printed on the router label. WPA2 provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select WPA-PSK [TKIP] + WPA2-PSK [AES] security.
 - **WPA-PSK [TKIP] + WPA2-PSK [AES]**. This type of security enables WiFi devices that support either WPA or WPA2 to join the router's WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps.
 - **WPA/WPA2 Enterprise**. This type of security requires that your WiFi network can access a RADIUS server. For more information, see [Set up WPA/WPA2 enterprise WiFi security](#) on page 90.
 - **WEP**. This is a legacy security option that is available in the 2.4 GHz band only if the selection from the **Mode** menu in the Wireless Network (2.4GHz b/g/n) section

is **Up to 54 Mbps** (see [Change the WiFi Mbps settings](#) on page 94). For more information about WEP security, see [Set up WEP legacy WiFi security](#) on page 92. However, we recommend that you use WPA2-PSK [AES] security.

- **None.** An open WiFi network that does not provide any security. Any WiFi device can join the WiFi network. We recommend that you do *not* use an open WiFi network because it doesn't provide any protection.

7. Click the **Apply** button.

Your settings are saved.

8. Make sure that you can reconnect over WiFi to the network with its new settings.

If you cannot connect over WiFi, check the following:

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

Set up WPA/WPA2 enterprise WiFi security

WPA/WPA2 enterprise WiFi security is typically used in business settings, not in home networks. To enable the router to provide WPA and WPA2 enterprise WiFi security, the router must be able to access a RADIUS server. Remote Authentication Dial In User Service (RADIUS) is an enterprise-level method for centralized Authentication, Authorization, and Accounting (AAA) management.

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

To set up WPA and WPA2 enterprise security:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Wireless**.
The Wireless Setup page displays.
5. In the Wireless Network (2.4GHz b/g/n) section or the Wireless Network (5GHz a/n/ac) section, select the **WPA/WPA2 Enterprise** Security Options radio button.
The page displays the WPA/WPA2 Enterprise section.
6. Enter the following settings:
 - **Encryption mode.** From the Encryption Mode menu, select the enterprise mode:
 - **WPA [TKIP] +WPA2 [AES].** This type of security enables WiFi devices that support either WPA or WPA2 to join the router's WiFi network. This is the default mode.
 - **WPA2 [AES].**WPA2 provides a secure connection but some older WiFi devices do not detect WPA2 and support only WPA. If your network includes such older devices, select WPA [TKIP] + WPA2 [AES] security.
 - **Group Key Update Interval.** Enter the interval in seconds after which the RADIUS group key is updated. The default interval is 3600 seconds.
 - **RADIUS server IP Address.** Enter the IPv4 address of the RADIUS server to which the WiFi network can connect.
 - **RADIUS server Port.** Enter the number of the port on the router that is used to access the RADIUS server for authentication. The default port number is 1812.
 - **RADIUS server Shared Secret.** Enter the shared secret (RADIUS password) that is used between the router and the RADIUS server during authentication of a WiFi user.
7. Click the **Apply** button.
Your settings are saved.

8. Make sure that you can reconnect over WiFi to the network with its new settings.

If you cannot connect over WiFi, check the following:

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

Set up WEP legacy WiFi security

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

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

To set up WEP security:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Wireless**.
The Wireless Network page displays.
5. From the **Mode** menu, select **Up to 54 Mbps**.

The page adjusts to display the **WEP** radio button.

6. Click the **Apply** button.
Your settings are saved.
7. Do one of the following:
 - **Set up WEP security for your WiFi network.** Continue with [Step 8](#).
 - **Set up WEP security for the guest WiFi network.** Do the following:
 - a. Select **Guest Network**.
The Guest Network Settings page displays.
 - b. Continue with [Step 8](#).
8. In the Security Options section, select the **WEP** radio button.
The page adjusts.
9. From the **Authentication Type** menu, select one of the following types:
 - **Automatic.** Clients can use either Open System or Shared Key authentication.
 - **Shared Key.** Clients can use only Shared Key authentication.
10. From the **Encryption Strength** menu, select the encryption key size:
 - **64-bit.** Standard WEP encryption, using 40/64-bit encryption.
 - **128-bit.** Standard WEP encryption, using 104/128-bit encryption. This selection provides higher encryption security.
11. Specify the active key by selecting the **Key 1**, **Key 2**, **Key 3**, or **Key 4** radio button.
Only one key can be the active key. To join the router's WiFi network, a user must enter the key value for the key that you specified as the active key.
12. Enter a value for the key:
 - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0-9, A-F). The key values are not case-sensitive.
 - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0-9, A-F). The key values are not case-sensitive.
13. Click the **Apply** button.
Your settings are saved.
14. Make sure that you can reconnect over WiFi to the network with its new settings.

If you cannot connect over WiFi, check the following:

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

Change the WiFi Mbps settings

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

To change the WiFi Mbps settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Wireless**.
The Wireless Setup page displays.
5. For the 2.4 GHz WiFi band, in the Wireless Network (2.4GHz b/g/n) section, select a setting from the **Mode** menu:
 - **Up to 600 Mbps**. Performance mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network in the 2.4 GHz band and allows 802.11n devices to function at up to 600 Mbps. This mode is the default mode.

- **Up to 289 Mbps.** Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network in the 2.4 GHz band but limits 802.11n devices to functioning at up to 289 Mbps.
 - **Up to 54 Mbps.** Legacy mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network in the 2.4 GHz band but limits 802.11n devices to functioning at up to 54 Mbps.
6. For the 5 GHz WiFi band, in the Wireless Network (5GHz a/n/ac) section, select a setting from the **Mode** menu:
- **Up to 1625 Mbps.** Performance mode. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the network in the 5 GHz band and allows 802.11ac devices to function at up to 1625 Mbps. This mode is the default mode.
 - **Up to 750 Mbps.** Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the network in the 5 GHz band but limits 802.11ac devices to functioning at up to 750 Mbps.
 - **Up to 360 Mbps.** Legacy mode. This mode allows 802.11ac, 802.11n, and 802.11a devices to join the network in the 5 GHz band but limits 802.11ac and 802.11n devices to functioning at up to 300 Mbps.
7. Click the **Apply** button.
Your settings are saved.

Change the transmission power of the WiFi radios

By default, your router's radio transmission power is set to 100%. This allows your router to give you the largest WiFi coverage. If you need WiFi coverage for a particular area or room only, and you also want to save power consumption while using your router, you can lower the transmission power of your router.

To change the transmission power:

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

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

The BASIC Home page displays.

4. Select **Wireless**.

The Wireless Setup page displays.

5. In the Wireless Network (2.4GHz b/g/n) section, select a percentage from the **Transmit Power Control** menu.

6. In the Wireless Network (5GHz a/n/ac) section, select a percentage from the **Transmit Power Control** menu.

7. Click the **Apply** button.

Your settings are saved.

Set up a guest WiFi network

A guest network lets you share your Internet connection with visitors without telling them your WiFi security password. You can create a different WiFi password for the guest network. The guest network WiFi mode and channel settings are the same as your 2.4 GHz and 5 GHz WiFi networks.

By default, the guest WiFi network is disabled. You can set up the guest WiFi network for each WiFi band. The router simultaneously supports the 2.4 GHz band for 802.11n, 802.11g, and 802.11b devices and the 5 GHz band for 802.11ac, 802.11n, and 802.11a devices.

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

- **2.4 GHz guest WiFi network SSID.** NETGEAR_Guest
- **5 GHz guest WiFi network SSID.** NETGEAR-5G_Guest

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

To set up a guest network:

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

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

The BASIC Home page displays.

4. Select **Guest Network**.

The Guest Network Settings page displays.

5. Enter the following settings to set up a 2.4 GHz or 5 GHz guest WiFi network:

- **Enable Guest Network.** By default, the guest WiFi network is disabled. To enable the guest WiFi network, 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 guest WiFi network, clear the **Enable SSID Broadcast** check box.
- **Allow guests to see each other and access my local network.** By default, guests who are connected to the guest WiFi network cannot access WiFi devices or Ethernet devices that are connected to your WiFi network. To allow access to your 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 guest WiFi network name. The default 2.4 GHz SSID is NETGEAR_Guest. The default 5 GHz SSID NETGEAR-5G_Guest.
To change the SSID, enter a 32-character (maximum), case-sensitive name in this field.

6. Select a WiFi security option for the 2.4 GHz or 5 GHz guest WiFi network:

- **WPA2-PSK [AES].** WPA2 provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. Select WPA2-PSK [AES] security to allow 802.11n devices to connect to guest WiFi network at the fastest speed. If your network includes older devices that do not support WPA2, select WPA-PSK [TKIP] + WPA2-PSK [AES] security. To use WPA2 security, in the **Password (Network Key)** field, enter a phrase of 8 to 63 characters. To join the guest WiFi network, the guest must enter this password.
- **WPA-PSK [TKIP] + WPA2-PSK [AES].** This type of security enables WiFi devices that support either WPA or WPA2 to join the 2.4 GHz band of the guest WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps. To use WPA + WPA2 security, in the **Password (Network Key)** field, enter a phrase of 8 to 63 characters. To join the guest WiFi network, the guest must enter this password.
- **WEP.** This is a legacy security option that is available in the 2.4 GHz band only if the selection from the **Mode** menu in the Wireless Network (2.4GHz b/g/n) section

on the Wireless Setup page the is **Up to 54 Mbps** (see [Change the WiFi Mbps settings](#) on page 94). For more information about WEP security, see [Set up WEP legacy WiFi security](#) on page 92. However, we recommend that you use WPA2-PSK [AES] security.

- **None.** An open WiFi network that does not provide any security. Any WiFi device can join the guest WiFi network. This is the default setting for the guest WiFi network.

7. Click the **Apply** button.

Your settings are saved.

8. Make sure that you can reconnect over WiFi to the network with its new security settings.

If you cannot connect over WiFi, check the following:

- Is your computer or mobile device already connected to another WiFi network in your area? If so, disconnect it from that WiFi network and connect it to the WiFi network that the router provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
- Does your computer or mobile device display as an attached device? If it does, it is connected to the network.
- Are you using the correct network name (SSID) and password?

Control the WiFi radios

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

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

Use the WiFi On/Off button

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

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

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

Enable or disable the WiFi radios

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

To enable or disable the WiFi radios:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
The Wireless Settings page displays.
5. Do one of the following for your router's WiFi networks:
 - **Turn off the WiFi radio.** Clear the **Enable Wireless Router Radio** check box.
 - **Turn on the WiFi radio.** Select the **Enable Wireless Router Radio** check box.
6. Click the **Apply** button.
Your settings are saved.

Set up a WiFi schedule

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

To set up the WiFi schedule:

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

Manage WPS settings

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

To manage WPS settings:

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

The BASIC Home page displays.

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

The Wireless Settings page displays.

5. Scroll down to the WPS Settings section in the lower part of the page.

The Router's PIN field displays the fixed PIN that you use to configure the router's WiFi settings from another device through WPS.

6. (Optional) Select or clear the **Enable Router's PIN** check box.

By default, the **Enable Router's PIN** check box is selected and the router's PIN is enabled. For enhanced security, you can disable the router's PIN by clearing the **Enable Router's PIN** check box. However, when you disable the router's PIN, WPS is not disabled because you can still use the physical **WPS** button.

Note: The PIN function might temporarily be disabled if the router detects suspicious attempts to break into the router's WiFi settings by using the router's PIN through WPS. If this situation occurs, you can manually enable the PIN function by selecting the **Enable Router's PIN** check box. You can configure the number of times a failed PIN connection is allowed before the PIN function is disabled. (The default is three failed PIN connections.)

7. (Optional) Select or clear one or both of the **Keep Existing Wireless Settings** check boxes.

By default, both **Keep Existing Wireless Settings** check boxes are selected. We recommend that you leave these check boxes selected.

If you clear a check box, the next time a new WiFi client uses WPS to connect to the router, the router's WiFi settings for the radio band change to an automatically generated random SSID and passphrase. Clear a **Keep Existing Wireless Settings** check box only if you want to allow the WPS process to change the associated SSID and passphrase for WiFi access in the radio band.

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

8. Click the **Apply** button.

Your settings are saved.

Enable or disable implicit beamforming

Implicit beamforming means that the router can use information from WiFi clients that support beamforming to improve the WiFi signal.

To enable or disable implicit beamforming:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
The Wireless Settings page displays.
5. Scroll down below the WPS Settings section and select or clear the **Enable Implicit BEAMFORMING** check box.
Selecting this check box enables implicit beamforming. Clearing this check box disables implicit beamforming.
6. Click the **Apply** button.
Your settings are saved.
If you connected over WiFi to the network, you are disconnected from the network and must reconnect.

Enable or disable airtime fairness

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

To enable or disable airtime fairness:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Wireless Settings**.
The Wireless Settings page displays.
5. Scroll down below the WPS Settings section and select or clear the **Enable AIRTIME FAIRNESS** check box.
Selecting this check box enables airtime fairness. Clearing this check box disables airtime fairness.
6. Click the **Apply** button.
Your settings are saved.

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

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, and they must be connected to a 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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.

The BASIC Home page displays.

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

The Wireless Settings page displays.

5. Scroll down below the WPS Settings section and select or clear the **Enable MU-MIMO** check box.

Selecting this check box enables MU-MIMO. Clearing this check box disables MU-MIMO.

6. Click the **Apply** button.

Your settings are saved.

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

Manage advanced WiFi settings

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

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

To manage the advanced WiFi settings:

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

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

A login window opens.

3. Enter the router admin user name and password.

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

The BASIC Home page displays.

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

The Wireless Settings page displays.

5. Change the settings for 2.4 GHz or 5 GHz WiFi network.

CAUTION: These settings are reserved for WiFi testing and advanced configuration only. Do not change these settings unless directed by NETGEAR support or unless you are sure what the consequences are. Incorrect settings might disable the WiFi function of the router unexpectedly.

- **Fragmentation Length (256-2346).** The default is 2346.
- **CTS/RTS Threshold (1-2347).** The default is 2347.
- **Preamble Mode.** The default is Long Preamble.

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

8

Manage Your Router

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

The chapter includes the following sections:

- [Update the router firmware](#)
- [Change the admin password](#)
- [Enable admin password recovery](#)
- [Recover the admin password](#)
- [Manage the router configuration file](#)
- [View information about the router and the Internet and WiFi settings](#)
- [Display the statistics of the Internet port](#)
- [Check the Internet connection status](#)
- [View and manage logs of router activity](#)
- [View devices currently on the network](#)
- [Monitor, meter, and control Internet traffic](#)
- [Set your time zone](#)
- [Change the NTP server](#)
- [Disable LED blinking or turn off LEDs](#)
- [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 load a specific firmware version to your router.

Check for new firmware and update the router

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

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

To check for new firmware and update your router:

1. Launch a web browser from a computer that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Administration > 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 **Yes** button.
The router locates and downloads the firmware and begins the update.

Note: To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting. After the router restarts, the top right on any page displays the new firmware version.

Manage the firmware update settings

You can manage whether the router automatically updates to future firmware versions as they become available.

To manage whether the router automatically updates to 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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Administration > 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.
 - **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.

Manually upload firmware to the router

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

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

To manually upload a firmware file to your router:

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

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

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

Note: To avoid the risk of corrupting the firmware, do not interrupt the update. For example, do not close the browser, click a link, or load a new page. Do not turn off the router. Wait until the router finishes restarting. After the router restarts, the top right on any page displays the new firmware version.

Change the admin password

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

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

To change the password for the admin user name:

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

Enable admin password recovery

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

To enable password recovery:

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

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

Recover the admin password

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

To recover your router admin password:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Click the **Cancel** button.
If password recovery is enabled, you are prompted to enter the serial number of the router.
The serial number is on the router label.
4. Enter the serial number of the router.
5. Click the **Continue** button.
A window opens requesting the answers to your security questions.
6. Enter the saved answers to your security questions.
7. Click the **Continue** button.
A window opens and displays your recovered password.
8. Click the **Login again** button.
A login window opens.
9. With your recovered password, log in to the router.

Manage the router configuration file

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

Back up the settings

To back up the router's configuration settings:

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

Restore the settings

To restore configuration settings that you backed up:

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

WARNING: Do not interrupt the restoration process.

View information about the router and the Internet and WiFi settings

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

To view information about the router and the Internet, modem, and WiFi settings:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Click the **ADVANCED** tab.
The ADVANCED Home page displays.
The information on this page uses the following color coding:
 - A green icon indicates that the Internet connection is fine and no problems exist. For a WiFi network, the network is enabled and secured.
 - A red icon indicates that configuration problems exist for the Internet connection or the connection is down. For a WiFi network, the network is disabled or down.
 - An amber icon indicates that the Internet port is configured but cannot get an Internet connection (for example, because the cable is disconnected), that a WiFi network is enabled but unprotected, or that another situation that requires your attention occurred.

Display the statistics of the Internet port

To display the statistics of the Internet port:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Click the **ADVANCED** tab.
The ADVANCED Home page displays.
5. In the Internet Port pane, click the **Show Statistics** button.
The Show Statistics window opens and displays following information:
 - **System Up Time**. The time elapsed since the router was last restarted.
 - **Port**. The statistics for the WAN (Internet) port, LAN (Ethernet) ports, and WLANs. For each port, the window displays the following information:
 - **Status**. The link status of the port.
 - **TxPkts**. The number of packets transmitted on this port since the router was last started.
 - **RxPkts**. The number of packets received on this port since the router was last started.
 - **Collisions**. The number of collisions on this port since the router was last started.
 - **Tx B/s**. The current transmission (outbound) bandwidth used on the WAN and LAN ports.
 - **Rx B/s**. The current reception (inbound) bandwidth used on the WAN and LAN ports.
 - **Up Time**. The time elapsed since this port acquired the link.
 - **Poll Interval**. The interval at which the statistics are updated on this page.

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

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

Check the Internet connection status

To check the Internet connection status:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Click the **ADVANCED** tab.
The ADVANCED Home page displays.
5. In the Internet Port pane, click the **Connection Status** button.
The Connection Status window opens. The information that displays depends on the type of Internet connection.

For example, if your Internet connection does not require a login and the router receives an IP address automatically, the window displays the following information:

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

6. To release (stop) the Internet connection, click the **Release** button.
7. To renew (restart) the Internet connection, click the **Renew** button.
8. To exit the screen, click the **Close Window** button.

View and manage logs of router activity

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

To view and manage logs:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The 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**. The name or IP address of the website or news group visited or to which access was attempted.
 - **Date and time**. The date and time the log entry was recorded.Other information might be displayed.
5. To customize the logs, scroll down and clear or select the check boxes in the Include in Log section.
6. To refresh the log screen, click the **Refresh** button.
7. To clear the log entries, click the **Clear Log** button.
8. To email the log immediately, click the **Send Log** button.

You must set up email notifications in order to receive the logs. The router to emails the logs to the address that you specified when you set up email notifications. For more information, see [Set up security event email notifications](#) on page 57.

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

View devices currently on the network

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

To view devices on the network:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **Attached Devices**.
The following information is displayed:
 - **Connection Type**. Wired or the WiFi band for the connection.
 - **Device Name**. If the device name is known, it is shown here.
 - **IP Address**. The IP address that the router assigned to this device when it joined the network. This address can change if a device is disconnected and rejoins the network.
 - **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label of the device.
5. To update this page, click the **Refresh** button.

Monitor, 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 restrictions

You can monitor the traffic volume without setting a limit.

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

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

Restrict Internet traffic by volume

You can record and restrict the traffic by volume in MB. This is useful when your ISP measures your traffic in volume.

To record and restrict the Internet traffic by volume:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Traffic Meter**.
The Traffic Meter page displays.
5. Select the **Enable Traffic Meter** check box.
6. Select the **Traffic volume control by** radio button.
7. From the corresponding menu, select an option:
 - **Download only**. The restriction is applied to incoming traffic only.
 - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
8. In the **Monthly Limit** field, enter how many MBytes (MB) per month are allowed.
9. If your ISP charges you for extra data volume when you make a new connection, enter the extra data volume in MB in the **Round up data volume for each connection by** field.
10. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
11. In the Traffic Control section, enter a value in minutes to specify when the router issues a warning message before the monthly limit in hours is reached.
This setting is optional. The router issues a warning when the balance falls below the number of minutes that you enter. By default, the value is 0 and no warning message is issued.
12. Select one or more of the following actions to occur when the limit is reached:
 - **Turn the Internet LED to flashing white/amber**. This setting is optional. When the traffic limit is reached, the Internet LED blinks alternating white and amber.

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

13. Click the **Apply** button.

Your settings are saved and the router restarts.

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

Restrict Internet traffic by connection time

You can record and restrict the traffic by connection time. This is useful when your Internet service provider (ISP) measures your connection time.

To record and restrict the Internet traffic by connection time:

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

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

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

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

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

This setting is optional. The router issues a warning when the balance falls under the number of minutes that you enter. By default, the value is 0 and no warning message is issued.

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

Your settings are saved and the router restarts.

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

View the Internet traffic volume and statistics

If you enabled the traffic meter, you can view the Internet traffic volume and statistics.

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

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

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

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

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

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

The Internet Traffic Statistics section displays when the traffic counter was started and what the traffic balance is. The table displays information about the connection time and traffic volume in MB.
6. To refresh the information 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 Internet service provider (ISP) set a traffic limit, your ISP might charge you for the overage traffic.

To unblock the traffic meter:

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

Set your time zone

To set your time zone:

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

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

The 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.

Change the NTP server

By default, the router uses the NETGEAR NTP server to sync the network time. You can change the NTP server to your preferred NTP server.

To change the NTP server to your preferred NTP server:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Administration > NTP Settings**.
The NTP Settings page displays.
5. Select the **Set your preferred NTP server** radio button.
6. Enter the NTP server domain name or IP address in the **Primary NTP server** field.
7. Click the **Apply** button.
Your settings are saved.

Disable LED blinking or turn off LEDs

The LEDs on the top panel of the router indicate activities and behavior. You can disable LED blinking for network communications, or turn off all LEDs except the Power LED.

To disable 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 opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > LED Control Settings**.
The LED Control Settings page displays.
5. To disable blinking, select the **Disable blinking on Internet LED, LAN LED, Wireless LED and USB LED when data traffic is detected** radio button.
6. To turn off all LEDs except the Power LED, select the **Turn off all LEDs except Power LED** radio button.
7. Click the **Apply** button.
Your settings are saved.

Return the router to its factory default settings

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

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

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

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

Use the Reset button

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

To reset the router to factory default settings:

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

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

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

Erase the settings

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

To erase the settings:

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

5. Click the **Erase** button.

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

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

9

Share USB Storage Devices Attached to the Router

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

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

The chapter contains the following sections:

- [USB device requirements](#)
- [Connect a USB storage device to the router](#)
- [Access a storage device connected to the router](#)
- [Back up Windows-based computers with ReadySHARE Vault](#)
- [Enable FTP access within your network](#)
- [View network folders on a storage device](#)
- [Add a network folder on a USB storage device](#)
- [Edit a network folder on a USB storage device](#)
- [Approve a USB storage device](#)
- [Remotely access a USB device using ReadyCLOUD](#)
- [Safely remove a USB storage device](#)

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

USB device requirements

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

kb.netgear.com/app/answers/detail/a_id/18985/~/readyshare-usb-drives-compatibility-list.

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

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

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

Connect a USB storage device to the router

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

To connect a USB device:

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

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

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

Access a storage device connected to the router

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

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

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

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

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

3. Select **Start > Run**.
4. Enter **\\readyshare** in the dialog box.
5. Click the **OK** button.
A window automatically opens and displays the files and folders on the USB storage device.

Map a USB device to a Windows network drive

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

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

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

3. Select **Start > Run**.
4. Enter **\\readyshare** in the dialog box.

5. Click the **OK** button.
A window automatically opens and displays the USB storage device.
6. Right-click the USB device and select **Map network drive**.
The Map Network Drive window opens.
7. Select the drive letter to map to the new network folder.
8. Click the **Finish** button.
The USB storage device is mapped to the drive letter that you specified.
9. To connect to the USB storage device as a different user, select the **Connect using different credentials** check box, click the **Finish** button, and do the following:
 - a. Type the user name and password.
 - b. Click the **OK** button.

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

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

To access the device from a Mac:

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

When you connect the USB storage device to the router's port, it might take up to two minutes before it is ready for sharing. By default, the USB storage device is available to all computers on your local area network (LAN).
3. On a Mac that is connected to the network, select **Go > Connect to Server**.
The Connect to Server window opens.
4. In the **Server Address** field, enter **smb://readyshare**.
5. When prompted, select the **Guest** radio button.
If you set up access control on the router and you allowed your Mac to access the network, select the **Registered User** radio button and enter **admin** for the name and router admin password for the password. For more information about access control, see [Enable access control to allow or block access to the Internet](#) on page 51.

6. Click the **Connect** button.

A window automatically opens and displays the files and folders on the USB storage device.

Back up Windows-based computers with ReadySHARE Vault

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

The following operating systems support ReadySHARE Vault:

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

To back up your Windows-based computer:

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

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

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

3. Download ReadySHARE Vault from netgear.com/readystatechange and install it on each Windows-based computer.
4. Launch ReadySHARE Vault.
5. Use the dashboard or the **Backup** tab to set up and run your backup.

Enable FTP access within your network

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

To enable FTP access within your network:

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

View network folders on a storage device

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

To view network folders:

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

The USB Storage (Advanced Settings) page displays.

5. Scroll down to the Available Networks Folder section to view the following settings:
 - **Share Name.** If only one USB device is connected, the default share name is USB_Storage.
You can click the name or you can type it in the address field of your web browser. If Not Shared is shown, the default share was deleted and no other share for the root folder exists.
 - **Read Access and Write Access.** The permissions and access controls on the network folder. All-no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the router.
 - **Folder Name.** The full path of the network folder.
 - **Volume Name.** The volume name from the storage device.
 - **Total Space and Free Space.** The current utilization of the storage device.

Add a network folder on a USB storage device

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

To add a network folder:

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

6. Click the **Create Network Folder** button.

The Add Folder window opens.

If this window does not open, your web browser might be blocking pop-ups. If it is, change the browser settings to allow pop-ups.

7. From the **USB Device** menu, select the USB drive.

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

8. Click the **Browse** button and in the Folder field, select the folder.

9. In the **Share Name** field, type the name of the share.

10. From the **Read Access** menu and the **Write Access** menu, select the settings that you want.

All-no password (the default) allows all users to access the network folder. The other option is that only the admin user is allowed access to the network folder. The password for admin is the same one that you use to log in to the router.

11. Click the **Apply** button.

The folder is added on the USB storage device.

12. Click the **Close Window** button.

The window closes.

Edit a network folder on a USB storage device

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

To edit a network folder:

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

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

A login window opens.

3. Enter the router admin user name and password.

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

The BASIC Home page displays.

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

The USB Storage (Advanced Settings) page displays.

5. In the Available Network Folders section, select the USB storage device.

6. Click the **Edit** button.

The Edit Network Folder window opens.

7. Change the settings in the fields as needed.

8. Click the **Apply** button.

Your settings are saved.

Approve a USB storage device

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

To approve USB devices:

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

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

A login window opens.

3. Enter the router admin user name and password.

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

The BASIC Home page displays.

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

The USB Settings page displays.

By default the Enable any USB Device connection to the USB port radio button is selected. This setting lets you connect and access all your USB devices.

5. In the **Enable any USB Device connected to the USB port** section, select the **No** radio button.

6. Click the **Approved Devices** button.

The approved and available USB devices display.

7. In the Available USB Devices list, select the device that you want to approve.

8. Click the **Add** button.

The USB device is added to the Approved USB Devices list.

9. Select the **Allow only approved devices** check box.
10. Click the **Apply** button.
Your settings are saved.
11. To work with another USB storage device, first click the **Safely Remove USB Device** button for the currently connected USB storage device.
Connect the other USB device, and repeat this process.

Remotely access a USB device using ReadyCLOUD

NETGEAR ReadyCLOUD for routers lets you remotely access files stored on a USB storage device that is connected to the router. Before you can use ReadyCLOUD, you must create a ReadyCLOUD account and register your router.

A ReadyCLOUD app is also available for Windows computers, Android mobile devices, and iOS mobile devices. For more information about setting up ReadyCLOUD, see the *ReadyCLOUD for Routers User Manual*, which is available online at downloadcenter.netgear.com.

Create a ReadyCLOUD account

To create a ReadyCLOUD account:

1. Launch a web browser from a computer or mobile device.
2. Visit readycloud.netgear.com.
The ReadyCLOUD Welcome page displays.
3. Click the **Sign In** link.
The Sign In page displays.
4. Click the **Create Account** link.
The Create a MyNETGEAR account page displays.
5. Complete the fields to set up your account, and click the **Create** button.
You are now ready to register your router with your ReadyCLOUD account.

Register your router with ReadyCLOUD

After you create a ReadyCLOUD account, you must register your router with your ReadyCLOUD account.

To register your router with your ReadyCLOUD account:

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

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

The BASIC Home page displays.
6. Select **ADVANCED > USB Functions > ReadySHARE Storage > ReadyCLOUD**.
The ReadyCLOUD page displays.
7. Enter your ReadyCLOUD user name and password and click the **Register** button.
If you did not yet create a ReadyCLOUD account, see [Create a ReadyCLOUD account](#) on page 136.

The router is registered with ReadyCLOUD.

Note: If the router's Internet connection mode is set to **Dial on Demand**, the router automatically changes the connection mode to **Always On**. This change is required for ReadyCLOUD to remotely access the USB storage device.
8. After registration, visit readycloud.netgear.com.
9. Click the **Sign In** link, enter your ReadyCLOUD user name and password, and click the **Sign In** button.

The ReadyCLOUD page displays the router that you registered and the contents of the USB storage device that is connected to the router.

Safely remove a USB storage device

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

To remove a USB storage device safely:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > USB Functions > ReadySHARE Storage**.
The USB Storage (Advanced Settings) page displays.
5. In the Available Network Folders sections, select the USB storage device.
6. Click the **Safely Remove USB Device** button.
This takes the device offline.
7. Physically disconnect the USB storage device.

10

Use VPN to Access Your Network

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

The chapter includes the following sections:

- [Set up a VPN connection](#)
- [Manage Dynamic DNS for VPN connections](#)
- [Enable and configure OpenVPN on the router](#)
- [Install OpenVPN software](#)
- [LAN requirements for VPN connections](#)
- [Use a VPN tunnel on a Windows-based computer](#)
- [Use VPN to access your Internet service at home](#)

Set up a VPN connection

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

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

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

To use a DDNS service, register for an account with a host name (sometimes called a domain name). You use the host name to access your network. The router supports these accounts: NETGEAR, No-IP, and Dyn.

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

Manage Dynamic DNS for VPN connections

With Dynamic DNS, you or someone else can use the Internet to access your router over a VPN connection. You can create a new Dynamic DNS account or use an existing one.

Set up a new Dynamic DNS account

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.
The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select **NETGEAR**.

You can select another service provider.

7. Select the **No** radio button.
8. In the **Host Name** field, type the name that you want to use for your URL.
The host name is sometimes called the domain name. Your free URL includes the host name that you specify and ends with mynetgear.com. For example, specify *MyName.mynetgear.com*.
9. In the **Email** field, type the email address for your account.
10. In the **Password (6-32 characters)** field, type the password for your account.
11. Click the **Register** button.
12. Follow the onscreen instructions to register for your NETGEAR Dynamic DNS service.

Specify a DNS account that you already created

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

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

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Dynamic DNS**.
The Dynamic DNS page displays.
5. Select the **Use a Dynamic DNS Service** check box.
6. From the **Service Provider** menu, select your provider.
7. Select the **Yes** radio button.
The page adjusts and displays the **Show Status**, **Cancel**, and **Apply** buttons.
8. In the **Host Name** field, type the host name (sometimes called the domain name) for your account.

9. Depending on the type of service, specify either the user name of the email address:
 - **No-IP account or DynDNS account.** In the **User Name** field, type the user name for your account.
 - **NETGEAR account.** In the **Email** field, type the email address for your account.
10. In the **Password (6-32 characters)** field, type the password for your DDNS account.
11. Click the **Apply** button.
Your settings are saved.
12. To verify that your Dynamic DNS service is enabled in the router, click the **Show Status** button.
A message displays the Dynamic DNS status.

Change the Dynamic DNS settings

You can change the settings for your Dynamic DNS account.

To change your settings:

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

Enable and configure OpenVPN on the router

You must enable OpenVPN and specify the OpenVPN service settings on your router before you or someone else can set up a remote VPN connection using OpenVPN.

Note: After you configure OpenVPN on the router, make sure that the VPN configuration files are installed on the remote clients. If you make changes to the OpenVPN configuration on the router, the VPN configuration files that the remote clients use might change, requiring new VPN configuration files to be downloaded and installed on the remote clients.

To enable and configure OpenVPN on the router:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > VPN Service**.
The VPN Service page displays.
5. Select the **Enable VPN Service** check box.
We recommend that you use the default TUN mode and TAP mode settings. However, if you know that you need other settings, you can change the TUN mode and TAP mode settings by doing the following:
 - To change the TUN mode service type, select the **UDP** or **TCP** radio button.
 - To change the TUN mode service port, type the port number that you want to use in the field.
The default port number is 12973.
 - To change the TAP mode service type, select the **UDP** or **TCP** radio button.
 - To change the TAP mode service port, type the port number that you want to use in the field.
The default port number is 12974.

6. Specify how client VPN connections can be used on the router by selecting one of the following radio buttons:
 - **Auto.** The router automatically uses the VPN service only for necessary access, that is, the router allows access to sites and services that would not be accessible without a VPN connection. This is the default selection. However, if some sites or services are not accessible to the VPN client, or if a user cannot access some sites on the Internet, select another radio button.
 - **All sites on the Internet & Home Network.** The VPN client can access the Internet and all sites and services on the router network, that is, behind the router firewall. Accessing the Internet remotely through a VPN connection might be slower than accessing the Internet directly.
 - **Home Network only.** The VPN client can access all sites and services on the router network, that is, behind the router firewall, but cannot access the Internet.
7. Click the **Apply** button.

Your settings are saved. OpenVPN service is enabled on the router.

If you or someone else wants to establish a remote VPN connection to your router, make sure that OpenVPN software is downloaded and installed on the computer or mobile device that will be used for the remote VPN connection.

Install OpenVPN software

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

Install the OpenVPN client utility and VPN configuration files on a Windows-based computer

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

1. Visit openvpn.net/index.php/download/community-downloads.html, download the OpenVPN client utility for a Windows-based computer, and install it on the Windows-based computer.

You might need administrative privileges to install the OpenVPN client utility.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.

A login window opens.

4. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > VPN Service**.
The VPN Service page displays.
6. Make sure that the **Enable VPN Service** check box is selected.
For more information, see [Enable and configure OpenVPN on the router](#) on page 143.
7. In the OpenVPN configuration package download section, click the **For Windows** button, and download the router's VPN configuration files.
8. Unzip the configuration files and copy them to the folder in which the OpenVPN client utility is installed.
9. Modify the VPN interface name to NETGEAR-VPN by doing the following:
 - a. In Windows, open Network Connection or Network and Sharing Center.
The network connection information displays.
 - b. In the local area connection list, find the local area connection with the device name TAP-Windows Adapter.
 - c. Change the name of the associated local area connection to **NETGEAR-VPN**.
Make sure that you change the name of the local area connection, *not* the device name (TAP-Windows Adapter).

If you do not change the local area connection name, the VPN connection to the router will fail.

The computer is now ready to for you to set up a VPN connection to the router.

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

Install the OpenVPN client utility and VPN configuration files on a Mac

To download and install the OpenVPN client utility and the router's VPN configuration files on a Mac:

1. Visit code.google.com/p/tunnelblick/, download the OpenVPN client utility for a Mac, and install it on the Mac.
You might need administrative privileges to install the OpenVPN client utility.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.
A login window opens.
4. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > VPN Service**.
The VPN Service page displays.
6. Make sure that the **Enable VPN Service** check box is selected.
For more information, see [Enable and configure OpenVPN on the router](#) on page 143.
7. In the OpenVPN configuration package download section, click the **For MacOSX** button, and download the router's VPN configuration files.
8. Unzip the configuration files and copy them to the folder in which the OpenVPN client utility is installed.
The Mac is now ready to for you to set up a VPN connection to the router.
For more information about using OpenVPN on a Mac computer, visit openvpn.net/index.php/access-server/docs/admin-guides/183-how-to-connect-to-access-server-from-a-mac.html.

Install the OpenVPN client utility and VPN configuration files on an iOS device

To download and install the OpenVPN client utility and the router's VPN configuration files on an iOS device:

1. On your iOS device, visit the Apple app store and download and install the OpenVPN Connect app.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **<http://www.routerlogin.net>**.
A login window opens.
4. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > VPN Service**.
The VPN Service page displays.
6. Make sure that the **Enable VPN Service** check box is selected.
For more information, see [Enable and configure OpenVPN on the router](#) on page 143.
7. In the OpenVPN configuration package download section, click the **For Smart Phone** button, and download the router's VPN configuration files to your iOS device or computer.
If you download the configuration files to a computer, unzip the configuration files that you downloaded and send the files to your iOS device.
The configuration files include the `.ovpn` file.
8. On your iOS device, open the `.ovpn` file, select the OpenVPN Connect app, and import the `.ovpn` file.
Your iOS device is now ready to for you to set up a VPN connection to the router.
For more information about using OpenVPN on an iOS device, visit vpngate.net/en/howto_openvpn.aspx#ios.

Install the OpenVPN client utility and VPN configuration files on an Android device

To download and install the OpenVPN client utility and the router's VPN configuration files on an Android device:

1. On your Android device, visit the Google Play Store and download and install the OpenVPN Connect app.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.
A login window opens.
4. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > VPN Service**.
The VPN Service page displays.
6. Make sure that the **Enable VPN Service** check box is selected.
For more information, see [Enable and configure OpenVPN on the router](#) on page 143.
7. In the OpenVPN configuration package download section, click the **For Smart Phone** button, and download the router's VPN configuration files to your Android device or computer.
If you download the configuration files to a computer, unzip the configuration files that you downloaded and send the files to your Android device.
The configuration files include the `.ovpn` file.
8. On your Android device, start the OpenVPN Connect app, and search for and import the `.ovpn` file.
Your Android device is now ready for you to set up a VPN connection to the router.
For more information about using OpenVPN on an Android device, visit vpngate.net/en/howto_openvpn.aspx#android.

LAN requirements for VPN connections

For a VPN tunnel to work, the local LAN IP address of the remote router must use a different LAN IP scheme from that of the local LAN where your VPN client computer is connected. If both networks use the same LAN IP scheme, when the VPN tunnel is established, you cannot access your home router or your home network with the OpenVPN software.

The default LAN IP address scheme for the router is 192.x.x.x. The most common IP schemes are 192.x.x.x, 172.x.x.x, and 10.x.x.x. If you experience a conflict, change the IP scheme either for your home network or for the network with the client VPN computer.

Use a VPN tunnel on a Windows-based computer

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

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

1. Launch the OpenVPN application with administrator privileges.

The **OpenVPN** icon displays in the Windows taskbar.

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

2. Right-click the **OpenVPN** icon and select **Connect**.

The VPN connection is established. You can do the following:

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

Use VPN to access your Internet service at home

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

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

Allow VPN clients full Internet access

By default, the router is set up to allow VPN connections that are managed automatically. You can change the settings to allow full access to both your home Internet service and your home network. Accessing the Internet remotely through a VPN might be slower than accessing the Internet directly.

Note: For information about specifying PVN access in the router, see [Enable and configure OpenVPN on the router](#) on page 143. For information about installing OpenVPN software on your computer or mobile device, see [Install OpenVPN software](#) on page 144.

To allow VPN clients to full access to both your home Internet service and your home network:

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

For more information, see [Enable and configure OpenVPN on the router](#) on page 143.

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.

Use a VPN tunnel to access your Internet service at home

To access your Internet service:

1. Set up the router to allow VPN access to your Internet service.
See [Enable and configure OpenVPN on the router](#) on page 143.
2. On your computer or mobile device, launch the OpenVPN application.
If you use a Windows-based computer, the **OpenVPN** icon displays in the Windows taskbar.
3. Right-click the icon and select **Connect**.
4. When the VPN connection is established, launch your Internet browser.

Block Internet access for VPN clients

By default, the router is set up to allow VPN connections that are managed automatically. You can change the settings to block access to your home Internet service and allow access only to your home network.

To block Internet access for VPN clients:

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

The VPN Service page displays.

5. Make sure that the **Enable VPN Service** check box is selected.
For more information, see [Enable and configure OpenVPN on the router](#) on page 143.
6. Scroll down to the Clients will use this VPN connection to access section, and select the **Home Network only** radio button.
The VPN connection is only to your home network, not to the Internet service for your home network.
7. Click the **Apply** button.
Your settings are saved.

11

Manage Port Forwarding and Port Triggering Traffic Rules

As an advanced function of the firewall, you can use port forwarding and port triggering to set up port traffic rules for Internet services and applications. These rules apply specifically to ports. You need networking knowledge to set up port traffic rules.

This chapter includes the following sections:

- [Manage port forwarding to a local server for services and applications](#)
- [Manage port triggering for services and applications](#)

Manage port forwarding to a local server for services and applications

If a server is part of your network, you can allow certain types of incoming traffic to reach the server. For example, if your router supports such a configuration, 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.

Forward incoming traffic for a default service or application

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

To forward incoming traffic for a default service or application:

1. Decide which type of service, application, or game you want to provide.
 2. Find the local IP address of the computer on your network that will provide the service.
The server computer must always receive the same IP address. To specify this setting, you can use the reserved IP address feature.
 3. Launch a web browser from a computer or mobile device that is connected to the router network.
 4. Enter **http://www.routerlogin.net**.
A login window opens.
 5. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
 6. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
 7. Make sure that the **Port Forwarding** radio button is selected.
 8. From the **Service Name** menu, select the service or application.
If the service or application that you want to add is not in the list, create a port forwarding rule with a custom service or application (see [Add a port forwarding rule for a custom service or application](#) on page 155).
-

9. In the **Server IP Address** field, enter the IP address of the computer that must provide the service or that runs the application.
10. Click the **Add** button.
Your settings are saved and the rule is added to the table.

Add a port forwarding rule for a custom service or application

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

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

1. Find out which port number or range of numbers the service or application uses.
You can usually find this information by contacting the publisher of the service or application or through user groups or news groups.
2. Launch a web browser from a computer or mobile device that is connected to the router network.
3. Enter **http://www.routerlogin.net**.
A login window opens.
4. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
6. Make sure that the **Port Forwarding** radio button is selected.
7. Click the **Add Custom Service** button.
The Ports - Custom Services page displays.
8. Set up a new port forwarding rule for a custom service or application by specifying the following settings:
 - **Service Name**. Enter the name of the custom service or application.
 - **Protocol**. Select the protocol (**TCP** or **UDP**) that is associated with the service or application. If you are unsure, select **TCP/UDP**.

- **External port range.** If the service or application uses a single port, enter the port number in the **External port range** field. If the service or application uses a range or ranges of ports, specify the range in the **External port range** field. Specify one range by using a dash between the port numbers. Specify multiple ranges by separating the ranges with commas.

Note: You can enter a port range and fixed ports in one rule. For example, you can enter an external port range 30-50, 78, 100-102. If you enter an internal port range 40-60, 99, 200-202, this rule forwards traffic from external ports 30-50 to internal ports 40-60.

- **Internal port range.** Specify the internal port or ports by one of these methods:
 - If the external and internal port or ports are identical, leave the **Use the same port range for Internal port** check box selected.
 - If the service or application uses a single port, clear the check box and enter the port number in the **Internal port range** field.
 - If the service or application uses a range or ranges of ports, clear the check box and specify the range in the **Internal port range** field. Specify one range by using a dash between the port numbers. Specify multiple ranges by separating the ranges with commas.

Note: You can enter a port range and fixed ports in one rule. For example, you can enter an internal port range 40-60, 99, 200-202. If you enter an external port range 30-50, 78, 100-102, this rule forwards traffic from external ports 30-50 to internal ports 40-60.

- **Internal IP address.** Either enter an IP address in the **Internal IP address** field or select the radio button for an attached device that is listed in the table.

9. Click the **Apply** button.

Your settings are saved. The rule is added to the table on the Port Forwarding / Port Triggering page.

Change a port forwarding rule

You can change an existing port forwarding rule.

To change a port forwarding rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
5. Make sure that the **Port Forwarding** radio button is selected.
6. In the table, select the radio button for the service name.
7. Click the **Edit Service** button.
The Ports - Custom Services page displays.
8. Change the settings.
For information about the settings, see [Add a port forwarding rule for a custom service or application](#) on page 155.
9. Click the **Apply** button.
Your settings are saved. The changed rule displays in the table on the Port Forwarding / Port Triggering page.

Remove a port forwarding rule

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

To remove a port forwarding rule:

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

3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
5. Make sure that the **Port Forwarding** radio button is selected.
6. In the table, select the radio button for the service name.
7. Click the **Delete Service** button.
The rule is removed from the table.
A default rule remains available in the **Service Name** menu. A custom rule is removed. If you want to reinstate the custom rule, you must redefine it.

Application example: Make a local web server public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

To make a local web server public:

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation.
In this example, your router always gives your web server an IP address of 192.168.1.33.
2. On the Port Forwarding / Port Triggering page, configure the router to forward the HTTP service to the local address of your web server at **192.168.1.33**.
HTTP (port 80) is the standard protocol for web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and specify that name on the Dynamic DNS page of the router.
Dynamic DNS makes it much easier to access a server from the Internet because you can enter the name in the web browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

How the router implements a port forwarding rule

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

1. When you enter the URL `www.example.com` in your browser, the browser sends a web page request message with the following destination information:
 - **Destination address.** The IP address of `www.example.com`, which is the address of your router.
 - **Destination port number.** 80, which is the standard port number for a web server process.
2. The router receives the message and finds your port forwarding rule for incoming port 80 traffic.
3. The router changes the destination IP address in the message to `192.168.1.123` and sends the message to that computer.
4. Your web server at IP address `192.168.1.123` receives the request and sends a reply message to your router.
5. Your router performs Network Address Translation (NAT) on the source IP address and sends the reply through the Internet to the computer or mobile device that sent the web page request.

Manage port triggering for services and applications

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- An application must use port forwarding to more than one local computer (but not simultaneously).
- An application must open incoming ports that are different from the outgoing port.

With port triggering, the router monitors traffic to the Internet from an outbound “trigger” port that you specify. For outbound traffic from that port, the router saves the IP address of the computer that sent the traffic. The router temporarily opens the incoming port or ports that you specify in your rule and forwards that incoming traffic to that destination.

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

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance, make sure that Universal Plug-N-Play (UPnP) is enabled.

Add a port triggering rule

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

To add a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
The port triggering settings display.
6. Click the **Add Service** button.
The Port Triggering - Services page displays.
7. Set up a new port triggering rule with a custom service or application by specifying 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.
 - **Single address.** Restricts the service 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 must open the inbound ports.
 - **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 rule is added to the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page.

Change a port triggering rule

You can change an existing port triggering rule.

To change a port triggering rule:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Enter **http://www.routerlogin.net**.
A login window opens.
3. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
4. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
5. Select the **Port Triggering** radio button.
The port triggering settings display.
6. In the Port Triggering Portmap Table, select the radio button for the service name.
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 160.

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.

Specify the time-out for port triggering

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

To specify the time-out for port triggering:

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

Disable port triggering

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

To disable port triggering:

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

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

The BASIC Home page displays.

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

The Port Forwarding / Port Triggering page displays.

5. Select the **Port Triggering** radio button.

The port triggering settings display.

6. In the Port Triggering Portmap Table, select the radio button for the service name.

7. Click the **Delete Service** button.

The rule is removed from the Port Triggering Portmap Table. If you want to reinstate the rule, you must redefine it.

Application example: Port triggering for Internet Relay Chat

Some application servers, such as FTP and IRC servers, send replies to multiple port numbers. Using port triggering, you can tell the router to open more incoming ports when a particular outgoing port starts a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer."

The following sequence shows the effects of this port triggering rule:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and observing the destination port number of 6667, your router creates another session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (for example, port 33333) as the destination port and also sends an "identify" message to your router with destination port 113.
6. When your router receives the incoming message to destination port 33333, it checks its session table to see if a session is active for port number 33333. Finding an active

session, the router restores the original address information replaced by NAT and sends this reply message to your computer.

7. When your router receives the incoming message to destination port 113, it checks its session table and finds an active session for port 113 associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

12

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](#)
- [Troubleshoot with the LEDs](#)
- [You cannot log in to the router](#)
- [Resolve a browser security warning](#)
- [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. Turn off the router.
3. Plug in the modem and turn it on. Wait two minutes.
4. Turn on the router and wait two minutes.

Check the power adapter and Ethernet cable connections

If the router does not start, make sure that the power adapter cable is securely plugged in.

If the Internet connection or LAN connections do not function, make sure that the Ethernet cables are securely plugged in. The Internet LED on the router is lit if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on. If one or more powered-on computers are connected to the router by an Ethernet cable, the corresponding numbered router LAN port LEDs light.

Check the WiFi settings

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

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

Check the network settings

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

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

Troubleshoot with the LEDs

By default, the router uses standard LED settings.

Standard LED behavior when the router is powered on

After you turn on power to the router, verify that the following sequence of events occurs:

1. When power is first applied, verify that the Power LED is lit.
2. After about two minutes, verify the following:
 - The Power LED is lit.
 - The Internet LED is lit.
 - The WiFi LEDs are lit (unless you turned off the WiFi radios).

You can use the LEDs of the router for troubleshooting.

Power LED is off or blinking

This could occur for a number of reasons. Check the following:

- Make sure that the power adapter is securely connected to your router and securely connected to a working power outlet.
- Make sure that you are using the power adapter that NETGEAR supplied for this product.
- If the Power LED blinks slowly and continuously, the router firmware is corrupted. This can happen if a firmware update is interrupted, or if the router detects a problem with the firmware. If the error persists, it is likely that a hardware problem exists. For recovery instructions, or help with a hardware problem, contact Technical Support at netgear.com/support.

LEDs never turn off

When the router is turned on, the LEDs light for about 10 seconds and then turn off. If all the LEDs stay on, this indicates a fault within the router.

If all LEDs are still lit one minute after power-up, do the following:

- Cycle the power to see if the router recovers.
- Press and hold the **Reset** button to return the router to its factory settings.

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

Internet or Ethernet 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 LEDs are off

If the WiFi LEDs stay off, check to see if someone pressed the **WiFi On/Off** button on the router. This button turns the WiFi radios in the router on and off. If someone disabled the WiFi radios by using the router web interface, the WiFi LEDs also stay off. The WiFi LEDs are 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 you are using the correct login information. The user name is **admin**. The password is the one that you specified the first time that you logged in. (The default password is **password**.) The user name and password are case-sensitive. Make sure that Caps Lock is off when you enter this information.

- Try quitting the browser and launching it again.
- Make sure that Java, JavaScript, or ActiveX is enabled in your browser. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.
- Make sure that the IP address of your computer or mobile device is in the same subnet as the router. If you are using the recommended addressing scheme, the IP address of your computer or mobile device is in the range of 192.168.1.2 to 192.168.1.254.
- If the IP address of your computer or mobile device is shown as 169.254.x.x, the computer or mobile device could not reach the router's DHCP server and the Windows or Mac operating system generated and assigned an IP address. Such an autogenerated IP address is in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer or mobile device to the router, and reboot your computer or mobile device.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1.

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

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

Resolve a browser security warning

The router provides secure web access from your LAN. This means that web access is encrypted through *secure* HTTP (HTTPS) instead of regular HTTP.

This extra security requires your router to verify that <http://www.routerlogin.net> is safe, causing a security warning to display in your browser when you try to access that domain.

You can add a security certificate for <http://www.routerlogin.net> to your computer or mobile device. After you add the certificate your computer or mobile device saves this information and a warning no longer displays for <http://www.routerlogin.net>.

Google Chrome: add a security exception

To access the router web interface with Google Chrome and add a security exception:

1. Launch Chrome from a computer or mobile device that is connected to the router network.
 2. Enter **http://www.routerlogin.net**.
A security warning displays saying your connection is not private.
 3. Click **Advanced > Proceed to www.routerlogin.net (unsafe)**.
A login window opens.
 4. Enter the router admin user name and password.
The user name is **admin**. The default password is **password**. If you already logged in before, the password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
 5. Save the certificate for www.routerlogin.net to a file by doing the following:
 - a. Click the red triangle icon next to "Not secure" in your address bar.
 - b. Click **Certificate (Invalid)**.
 - c. Select the **Details** tab.
 - d. Select **Copy to File**.
An installation wizard displays.
 - e. Click **Next**.
 - f. Make sure that the default **DER encoded binary X.509 (.CER)** option is selected and click **Next**.
 - g. Click **Browse** and save the certificate on your device.
 - h. Click **Next > Finish > OK**.
 6. Navigate to the folder where you saved the certificate and double-click the file.
The General tab displays.
 7. Click **Install Certificate...**
An installation wizard displays.
 8. Click **Next**.
 9. Select the **Place all certificates in the following store** radio button.
 10. Click **Browse** and select **Trusted Root Certification Authorities**.
-

11. Click **OK > Next > Finish**.
12. Follow the prompts to install the certificate.

Note: If you enter your router's default IP address (192.168.1.1) instead of www.routerlogin.net, Chrome still displays a warning message when you log in. The reason is that the certificate that you installed corresponds only to the www.routerlogin.net domain name, not to the IP address.

Apple Safari: add a security exception

To access the router web interface with Apple Safari and add a security exception:

1. Launch Safari from a computer or mobile device that is connected to the router network.
2. Enter **<http://www.routerlogin.net>**.
A security warning displays saying that your connection is not private.
3. Click **Show Details > visit this website**.
You are prompted to decide if you want to proceed.
4. Click **Visit Website**.
5. Enter your Mac **user name** and **password** and click **Update Settings**.

Mozilla Firefox: add a security exception

To access the router web interface with Mozilla Firefox and add a security exception:

1. Launch Firefox from a computer or mobile device that is connected to the router network.
2. Enter **<http://www.routerlogin.net>**.
A security warning displays.
3. Click **Advanced > View Certificate**.
A login window opens.
4. Select the **Details** tab.
5. Click **Export**.
6. Navigate to a location where you want to save the certificate and click **Save**.
7. Navigate to the same location and double-click the certificate.
8. Click **Install Certificate...**

An installation window opens.

9. Click **Next**.
10. Make sure that the **Permanently store this exception** option is selected.
11. Click **Browse** and select **Trusted Root Certification Authorities**.
12. Click **OK > Next > Finish**.
13. Follow the prompts to install the certificate.

Note: If you enter your router's default IP address (192.168.1.1) instead of www.routerlogin.net, Firefox still displays a warning message when you log in. The reason is that the certificate that you installed corresponds only to the www.routerlogin.net domain name, not to the IP address.

Microsoft Internet Explorer: add a security exception

To access the router web interface with Microsoft Internet Explorer and add a security exception:

1. Launch Internet Explorer from a computer or mobile device that is connected to the router network.
2. Enter **<http://www.routerlogin.net>**.
A security warning displays.
3. Click **Continue to this website (not recommended)**.
A login window opens.
4. Enter the router admin user name and password.
The user name is **admin**. The default password is **password**. If you already logged in before, the password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Click the red shield icon next to "Certificate error" in your address bar.
6. Click **View Certificates**.
The General tab displays.
7. Click **Install Certificate**.

If the Install Certificate button is not visible, modify the browser security setting by doing the following:

- a. In the browser, click the **Tools** tab.
- b. Select Internet **Options > Security**.
- c. Clear the **Enable Protected Mode option**.
Note that after installing the certificate, you can reenable this setting.
- d. Click **Apply > OK**.
- e. Restart Internet Explorer.
- f. After restarting Internet Explorer, if necessary, repeat [Step 2](#) through [Step 7](#).

An installation wizard starts.

8. Click **Next**.
9. Select the **Place all certificates in the following store** radio button.
10. Click **Browse** and select **Trusted Root Certification Authorities**.
11. Click **OK > Next**.
12. Follow the prompts to install the certificate.

Note: If you enter your router's default IP address (192.168.1.1) instead of www.routerlogin.net, Internet Explorer still displays a warning message when you log in. The reason is that the certificate that you installed corresponds only to the www.routerlogin.net domain name, not to the IP address.

Microsoft Edge: add a security exception

To access the router web interface with Microsoft Edge and add a security exception:

1. Launch Edge from a computer or mobile device that is connected to the router network.
2. Enter **<http://www.routerlogin.net>**.
A security warning displays.
3. Click **Details > Go on to the webpage**.
4. Save the certificate for the website to a file by doing the following:
 - a. Click the red triangle icon next to "Certificate error" in your address bar.
 - b. Click **View Certificates**.
The Certificate Information tab displays.

- c. Click **Export to file** and save the certificate to a location.
5. Navigate to the location where you saved the certificate and double-click the certificate.
The General tab displays.
6. Click **Install Certificate**.
The installation wizard starts.
7. Click the **Place all certificates in the following store** radio button.
8. Click **Browse** and select **Trusted Root Certification Authorities**.
9. Click **Next**.
10. Follow the prompts to install the certificate.

Note: If you enter your router's default IP address (192.168.1.1) instead of www.routerlogin.net, Edge still displays a warning message when you log in. The reason is that the certificate that you installed corresponds only to the www.routerlogin.net domain name, not to the IP address.

You cannot access the Internet

If you can access your router but not the Internet, check to see if the router can obtain a WAN IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful using the router web interface.

To check the WAN IP address:

1. Launch a web browser from a computer or mobile device that is connected to the router network.
2. Select an external site such as <https://www.netgear.com/>.
3. Enter **http://www.routerlogin.net**.
A login window opens.
4. Enter the router admin user name and password.
The user name is **admin**. The password is the one that you specified the first time that you logged in. The user name and password are case-sensitive.
The BASIC Home page displays.
5. Click the **ADVANCED** tab.

The ADVANCED Home page displays.

6. Check to see that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router did not obtain an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your modem to recognize your new router by restarting your network. For more information, see [Sequence to restart your network](#) on page 167.

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (ISP) might require a login program. Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account as the account name on the Internet Setup page.
- If your ISP allows only one Ethernet MAC address to connect to Internet and checks for your computer's MAC address, do one of the following:
 - Inform your ISP that you bought a new network device and ask them to use the router's MAC address.
 - Configure your router to clone your computer's MAC address.

If your router obtained an IP address, but your computer does not load any web pages from the Internet, it might be for one or more of the following reasons:

- Your computer might not recognize any DNS server addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer, and verify the DNS address. You can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- The router might not be configured as the TCP/IP gateway on your computer. If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address.
- You might be running login software that is no longer needed. If your ISP provided a program to log you in to the Internet, you no longer need to run that software after installing your router.

Troubleshoot Internet browsing

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet, it might be for the following reasons:

- The traffic meter is enabled, and the limit was reached.
By configuring the traffic meter not to block Internet access when the traffic limit is reached, you can resume Internet access. If your Internet service provider (ISP) sets a usage limit, they might charge you for the overage.
- Your computer might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.
Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, restart your computer. Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.
- The router might not be configured as the default gateway on your computer. Restart the computer and verify that the router address (www.routerlogin.net) is listed by your computer as the default gateway address.

Changes are not saved

If the router does not save the changes that you make in the router web interface, do the following:

- When entering configuration settings, always click the **Apply** button before moving to another page or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. It is possible that the changes occurred, but the old settings might be in the web browser's cache.

Troubleshoot WiFi connectivity

If you are experiencing trouble connecting over WiFi to the router, try to isolate the problem:

- Does the WiFi device or computer that you are using find your WiFi network?
If not, check the WiFi LED on the router. If it is off, you can press the **WiFi On/Off** button on the router to turn the router WiFi radios back on.

If you disabled the router's SSID broadcast, then your WiFi network is hidden and does not display in your WiFi client's scanning list. (By default, SSID broadcast is enabled.)

- Does your WiFi device support the security that you are using for your WiFi network (WPA, WPA2, WPA and WPA2 enterprise security, or WEP)?
- If you want to view the WiFi settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, and select **BASIC > Wireless**.

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

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

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

Troubleshoot your network using the ping utility

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

Test the LAN path to your router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

To ping the router from a Windows-based computer:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

ping www.routerlogin.net

3. Click the **OK** button.

You see a message like this one:

Pinging <IP address > with 32 bytes of data

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, one of the following problems might be occurring:

- Wrong physical connections
For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.
Check to see that the appropriate LEDs are lit for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and router.
- Wrong network configuration
Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Test the path from a Windows-based computer to a remote device

To test the path from a Windows-based computer to a remote device:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the Windows Run window, type
ping -n 10 <IP address>

where <IP address> is the IP address of a remote device such as your ISP DNS server.

If the path is functioning correctly, messages display that are similar to those shown in [Test the LAN path to your router](#) on page 178.

3. If you do not receive replies, check the following:
 - Check to see that IP address of your router is listed as the default gateway for your computer. If DHCP assigns the IP configuration of your computers, this information is not visible in your computer Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
 - Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.

Nighthawk AC2300 Cybersecurity WiFi Router Model RS400

- Check to see that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name on the Internet Setup page.
- Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.

Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem. Some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If your ISP does this, configure your router to “clone” or “spoof” the MAC address from the authorized computer.

A

Supplemental Information

This chapter includes technical information about your router.

The chapter covers the following topics:

- [Factory settings](#)
- [Technical specifications](#)

Factory settings

You can return the router to its factory settings. Use the end of a paper clip or a similar object to press and hold the **Reset** button on the back of the router for at least seven seconds. The router resets and returns to the factory configuration settings shown in the following table.

Table 3. Factory default settings

Feature		Default setting
Router login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	Autosensing
Local network (LAN)	LAN IP	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	Pacific time
	DHCP starting IP address	192.168.1.2
	DHCP ending IP address	192.168.1.254
	DMZ	Disabled
Time adjusted for daylight saving time	Disabled	
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Table 3. Factory default settings (Continued)

Feature	Default setting	
WiFi	WiFi communication	Enabled
	SSID name	See router label
	Security	WPA2-PSK (AES)
	Broadcast SSID	Enabled
	Transmission speed	Auto ¹
	Country/region	United States in the US; otherwise, varies by region
	RF channel	2.4 GHz: Auto 5 GHz, worldwide: Channel 44 5 GHz, North America: Channel 153
	Operating mode	Up to 600 Mbps at 2.4 GHz Up to 1625 Mbps at 5 GHz

¹Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical specifications

Table 4. Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, L2TP, Dynamic DNS, UPnP, and SMB
Power adapter	North America: 100V, 50/60 Hz input UK, Australia: 220V, 50/60 Hz, input Europe: 100-240V, 50/60 Hz input All regions (output): 19V/3.16 ADC output
Dimensions	11.22 x 7.26 x 1.97 in. (285 x 184.5 x 50 mm)
Weight	1.65 lb (750 g)
Operating temperature	0° to 40°C (32° to 104°F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	FCC Part 15 Class B EN 55022 (CISPR 22), Class B C-Tick N10947

Nighthawk AC2300 Cybersecurity WiFi Router Model RS400

Table 4. Router specifications (Continued)

Feature	Description
LAN	Four RJ-45 ports, compatible with 10BASE-T, 100BASE-TX, and 1000BASE-T
WAN	One RJ-45 ports are compatible with 10BASE-T, 100BASE-TX, and 1000BASE-T
USB	One USB 3.0 (front panel) One USB 2.0 (rear panel)
WiFi	Maximum WiFi signal rate complies with the IEEE 802.11 standard. ²
Radio data rates	Automatic rate sensing
Data encoding standards	IEEE 802.11b/g/n 2.4 GHz 256 QAM support IEEE 802.11a/n/ac 5.0 GHz 256 QAM support
Maximum computers per WiFi network	Limited by the amount of WiFi network traffic generated by each node (typically 50-70 nodes).
Operating frequency range	Up to 600 Mbps @ 2.4 GHz 256 QAM Up to 1625 Mbps @ 5 GHz 11ac 256 QAM ³
802.11 security	WPA2-PSK [AES] WPA-PSK [TKIP] + WPA2-PSK [AES] WPA/WPA2 Enterprise WEP (legacy security)

²Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

³NETGEAR makes no express or implied representations or warranties about this product's compatibility with any future standards.