

NETGEAR®

AC1600 WiFi Cable Modem Router

Model C6250

User Manual



February 2016
202-11533-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at <https://my.netgear.com>. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website.

For product updates and web support, visit <http://support.netgear.com>.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at <http://support.netgear.com/general/contact/default.aspx>.

Compliance

For regulatory compliance information, visit <http://www.netgear.com/about/regulatory>.

See the regulatory compliance document before connecting the power supply.

Trademarks

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

Contents

Chapter 1 Hardware Overview and Setup

Introduction	9
Front Panel and Right Side Panel	10
Back Panel	12
Position Your Modem Router	13
Install and Activate Your Cable Modem	14
Cable the Modem Router	14
Activate Your Internet Service	15
Activate Your Internet Service with Comcast XFINITY	16
Perform a Speed Test	17
Cable the Modem Router to a Router and Use Bridge Mode	17

Chapter 2 Connect to the Network and Access the Modem Router

Connect to the Network	21
Connect to the Modem Router Through an Ethernet Cable	21
Join the WiFi Network of the Modem Router	21
Types of Logins and Access	22
Product Label	23
Access NETGEAR genie	23
Access the Modem Router with the NETGEAR genie App	25

Chapter 3 Customize the Internet Settings

View the Cable Initialization of the Modem Router	27
Change the Cable Connection Starting Frequency	28
View or Manually Set Up the IPv4 Internet Settings	30
Manage the MTU Size	32
MTU Concepts	32
Change the MTU Size	34

Chapter 4 Manage the Basic WiFi Network Settings

Manage the Basic WiFi Settings and WiFi Security of the Main Network	36
View or Change the Basic WiFi Settings	36
Configure WPA/WPA2 Enterprise WiFi Security	41
Configure WEP Legacy WiFi Security for the Main WiFi Network	43
Use the WPS Wizard to Add a Device to the WiFi Network	45
Use WPS with the Push Button Method	45
Use WPS with the PIN Method	47
Manage the Basic WiFi Settings and WiFi Security of the Guest Network	48

Set Up and Enable a Guest Network 48
Configure WEP Legacy WiFi Security for the Guest WiFi Network..... 52

Chapter 5 Secure Your Network

Set Up Parental Controls 55
Allow or Block Access to Your Network 58
 Enable and Manage Network Access Control 59
 Manage Network Access Control Lists 60
Block Keywords and Domains for HTTP Traffic 66
 Set Up Blocking 66
 Remove a Keyword or Domain from the Blocked List 67
 Remove All Keywords and Domains from the Blocked List 68
 Specify a Trusted Computer 68
Block Access to Services and Applications 69
 Block a Default Service 70
 Add and Block a Custom Service 72
 Change the Settings for a Blocked Service 74
 Remove a Blocked Service 74
Schedule When Security Features Are Active 75
 Set Up a Schedule 75
 Change a Schedule 77
 Remove a Schedule 77
Set Up Security Event Email Notification 78

Chapter 6 Manage the WAN and LAN Network Settings

Manage the WAN Security Settings 81
Set Up a Default DMZ Server 82
Manage the SIP Application-Level Gateway 83
Manage the Modem Router’s LAN IP Address Settings 84
Manage IP Address Reservation 85
 Reserve an IP Address 85
 Change a Reserved IP Address 87
 Remove an IP Address Reservation 87
Manage the IPv6 LAN Settings 88
Change the Modem Router’s Device Name 90
Manage the Built-In DHCP Server 90
Manage the DHCP Server Address Pool 91
Manage Universal Plug and Play 92

Chapter 7 Manage the Modem Router and Monitor Your Network

View the Status and Statistics of the Modem Router 96
 View the Cable Information and Internet Port and WiFi Status 96
View the Traffic Statistics 101
 View the Internet Port Connection Status and Release and
 Renew the Connection 103
View Devices Currently on the Network 104

View WiFi Channels in Your Environment	105
View WiFi Networks in Your Environment	107
View and Manage the Log	108
Change the Password	110
Manage the Device Settings File of the Modem Router	111
Back Up the Settings	111
Restore the Settings	112
Return the Modem Router to Its Factory Default Settings	113
Use the Reset Button	114
Erase the Settings	114
Reboot the Modem Router	115
Monitor and Meter Internet Traffic	116
Start the Traffic Meter Without Traffic Volume Restrictions	116
View the Traffic Statistics and Traffic Status	117
Restrict Internet Traffic	118
Unblock the Traffic Meter After the Traffic Limit Is Reached	120
Manage the Modem Router Remotely	120

Chapter 8 Share a Storage Device

USB Device Requirements	124
Connect a USB Device to the Modem Router	124
Access a Storage Device Connected to the Modem Router	125
Manage Access to a Storage Device	126
Enable FTP Access Within Your Network	128
View Network Folders on a Device	129
Add a Network Folder on a Storage Device	130
Change a Network Folder, Including Read and Write Access, on a USB Drive	132
Approve USB Devices	134
Safely Remove a USB Device	135
Enable the Media Server	136

Chapter 9 Share a USB Printer

Install the Printer Driver and Cable the Printer	139
Download the ReadySHARE Printer Utility	139
Install the ReadySHARE Printer Utility	139
Use the Shared Printer	141
View or Change the Status of a Printer	142
Use the Scan Feature of a Multifunction USB Printer	143
Change NETGEAR USB Control Center Settings	144
Change the NETGEAR USB Control Center Language	145
Specify the Time-Out	145

Chapter 10 Access Storage Devices Through the Internet

Set Up and Manage Dynamic DNS	147
Your Personal FTP Server	147
Set Up a New Dynamic DNS Account	148

Specify a DNS Account That You Already Created	149
Access Storage Devices Through the Internet	151
Set Up FTP Access Through the Internet	151
Access Storage Devices Through the Internet with FTP	153

Chapter 11 Manage the Advanced WiFi Network Settings

Control the WiFi Radios	155
Use the WiFi On/Off Button	155
Enable or Disable the WiFi Radios	155
Set Up a WiFi Schedule	156
Manage Beamforming	158
Manage the Advanced WiFi Settings	159
Manage WPS Settings	161
Manage the Advanced WiFi Features	162

Chapter 12 Manage Port Forwarding and Port Triggering

Manage Port Forwarding to a Local Server for Services, Applications, and Games	166
Forward Incoming Traffic for a Default Service or Application	166
Add a Port Forwarding Rule with a Custom Service or Application	167
Change a Port Forwarding Rule	169
Remove a Port Forwarding Rule	170
Application Example: Make a Local Web Server Public	171
How the Modem Router Implements the Port Forwarding Rule	172
Manage Port Triggering for Services, Applications, and Games	172
Add a Port Triggering Rule	173
Change a Port Triggering Rule	175
Disable or Remove a Port Triggering Rule	176
Specify the Time-Out Period for Port Triggering	177
Disable Port Triggering	178
Application Example: Port Triggering for Internet Relay Chat	178

Chapter 13 Diagnostics and Troubleshooting

Perform Diagnostics	181
Ping an IP Address	181
Trace a Route	182
Quick Tips for Troubleshooting	184
Troubleshoot with the LEDs	185
Power LED Is Off	185
Power LED Is Red	185
WiFi LED Is Off	186
Ethernet LED Is Off	186
You Cannot Log In to the Modem Router	186
View and Manage the Event Log	187
Troubleshoot the Internet Connection	188
Troubleshoot the Cable Link	188

Internet LED Is Off	189
Obtain an Internet IP Address	189
Troubleshoot Internet Browsing	190
Changes Are Not Saved	191
Troubleshoot the WiFi Connectivity	191
TCP/IP Network Not Responding	192
Test the LAN Path to Your Modem Router	192
Test the Path from Your Computer to a Remote Device	192

Appendix A Factory Default Settings and Specifications

Factory Default Settings	195
Technical and Environmental Specifications	197

Hardware Overview and Setup

1

This user manual is for the NETGEAR® AC1600 WiFi Cable Modem Router, Model C6250.

This chapter contains the following sections:

- *Introduction*
- *Front Panel and Right Side Panel*
- *Back Panel*
- *Position Your Modem Router*
- *Install and Activate Your Cable Modem*
- *Cable the Modem Router to a Router and Use Bridge Mode*

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

Note: In this user guide, the terms *wireless* and *WiFi* mean the same thing.

Note: In this user guide, the terms *cable Internet provider* and *cable service provider* mean the same thing.

Introduction

The AC1600 WiFi Cable Modem Router Model C6250, in this manual referred to simply as the modem router, provides you with an easy and secure way to set up a WiFi home network with fast access to the Internet over a cable network with support for up to 680 Mbps. It lets you block unsafe Internet content and applications and protects the devices that you connect to your home or guest network.

The modem router provides one coaxial cable connector, two 10/100/1000 LAN Gigabit Ethernet ports, and one USB 2.0 port. In addition, the modem router supports WiFi connection speeds up to¹ 300 Mbps in the 2.4 GHz band for 802.11n devices and up to 1300 Mbps in the 5 GHz band for 802.11ac devices. Both 2.4 GHz and 5 GHz bands can be active simultaneously.

For information about setting up your new modem router, see the *AC1600 WiFi Cable Modem Router Model C6250 Quick Start Guide* that comes in the package. This chapter provides supplemental information that might help you with the setup.

For optimal performance, keep the modem router vertical in the stand and do not detach the stand. Do not mount the modem router to a wall; it is not suitable for wall mounting. For more information, see *Position Your Modem Router* on page 13.

1. Actual data throughput and WiFi coverage will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate and WiFi coverage. NETGEAR makes no express or implied representations or warranties about this product's compatibility with any future standards.

Front Panel and Right Side Panel

The front panel contains status LEDs that let you verify status and connections. The right side panel contains two buttons.

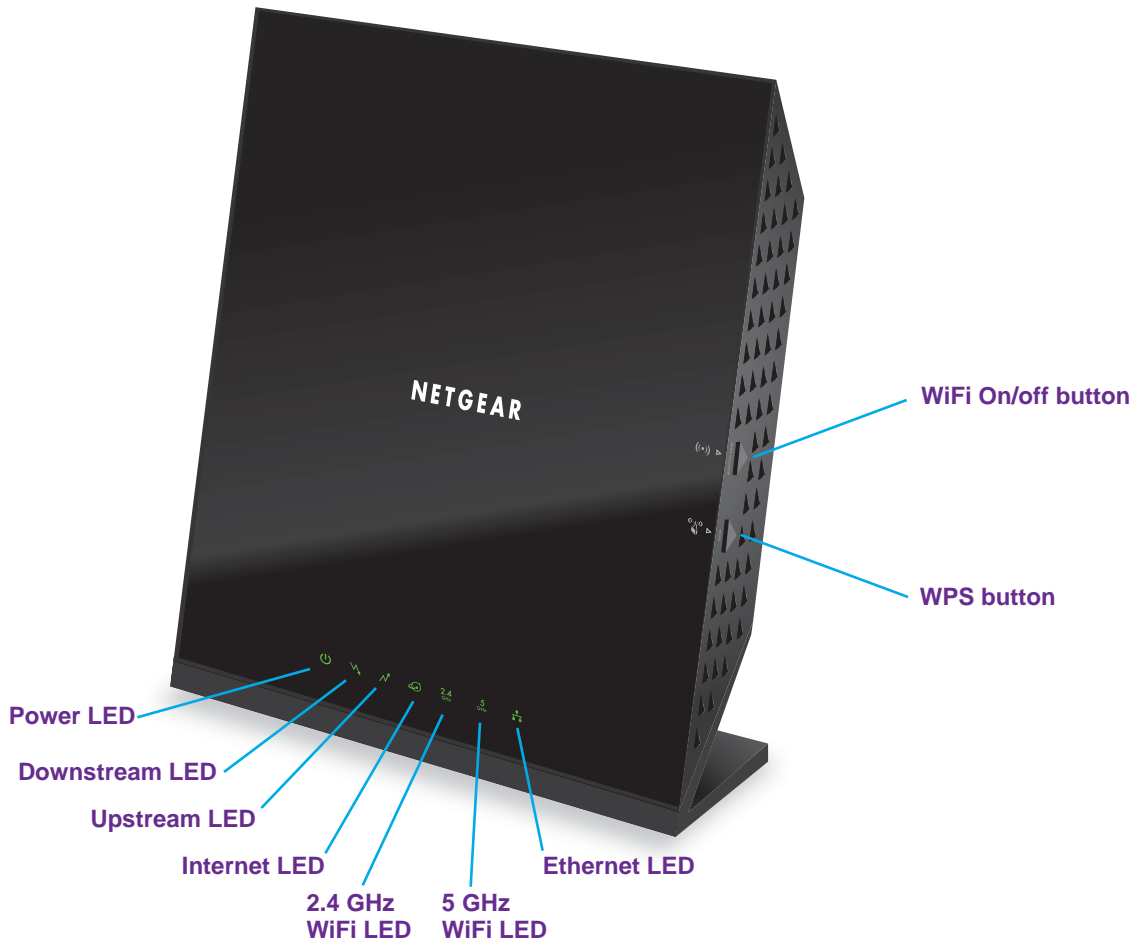









Figure 1. Front panel LEDs and side panel buttons



You can use the LEDs to verify status and connections. The following table lists and describes each LED on the front panel.

Table 1. Front panel LEDs

LED	Icon	Description
Power		<ul style="list-style-type: none"> • Solid green. Power is supplied to the modem router. • Off. No power is supplied to the modem router. • Solid red. The modem router is starting up (the Power LED lights solid red for a few seconds before turning green) or entered thermal cutoff mode. If the Power LED blinks red or lights solid red at any time other than when you turn it on, see Troubleshoot with the LEDs on page 185.
Downstream		<ul style="list-style-type: none"> • Solid amber. One downstream channel is locked. • Blinking amber. The modem router is scanning for a downstream channel. • Solid green. Two or more downstream channels are locked. • Blinking green. The modem router is scanning for additional downstream channels. • Off. No downstream channel is locked.
Upstream		<ul style="list-style-type: none"> • Solid amber. One upstream channel is locked. • Blinking amber. The modem router is scanning for an upstream channel. • Solid green. Two or more upstream channels are locked. • Blinking green. The modem router is scanning for additional upstream channels. • Off. No upstream channel is locked.
Internet		<ul style="list-style-type: none"> • Solid green. The modem router is online. • Blinking green. The modem router is synchronizing with the cable provider's cable modem termination system (CMTS). • Slow blinking amber and green. The modem router reached the traffic meter limit. (For information about the traffic meter, see Monitor and Meter Internet Traffic on page 116). • Off. The modem router is offline.
2.4 GHz WiFi LED		<ul style="list-style-type: none"> • Solid green. The 2.4 GHz radio is on. • Blinking green. The 2.4 GHz radio is transmitting or receiving data. • Blinking amber. WPS (Wi-Fi Protected Setup) is active. • Off. The 2.4 GHz radio is off.
5 GHz WiFi LED		<ul style="list-style-type: none"> • Solid green. The 5 GHz radio is on. • Blinking green. The 5 GHz radio is transmitting or receiving data. • Blinking amber. WPS (Wi-Fi Protected Setup) is active. • Off. The 5 GHz radio is off.
Ethernet		<ul style="list-style-type: none"> • Solid green. A device is connected to an Ethernet port and powered on. Each Ethernet port on the back panel provides two port LEDs (see Back Panel on page 12). • Blinking green. An Ethernet port is transmitting or receiving data. • Off. No device is connected to an Ethernet port.

The following table describes the buttons on the right side panel.

Table 2. Button descriptions

Button	Icon	Description
WiFi On/Off		By default, the 2.4 GHz and 5 GHz WiFi radios are enabled. Pressing this button for three seconds turns off both radios. Pressing the button again for three seconds turns on both radios. If you turn off the radios, both WiFi LEDs on the front panel turn off too. If you turn on the radios, both WiFi LEDs on the front panel light solid green.
WPS		Pressing this button for three seconds activates WPS (Wi-Fi Protected Setup) for two minutes to let you add a WiFi device to the WiFi network without typing the WiFi password. While WPS is active, both WiFi LEDs on the front panel blink amber. For more information about using WPS, see the following sections: <ul style="list-style-type: none"> • Join the WiFi Network of the Modem Router on page 21 • Use the WPS Wizard to Add a Device to the WiFi Network on page 45

Back Panel

The back panel contains ports, connectors, and a recessed button.

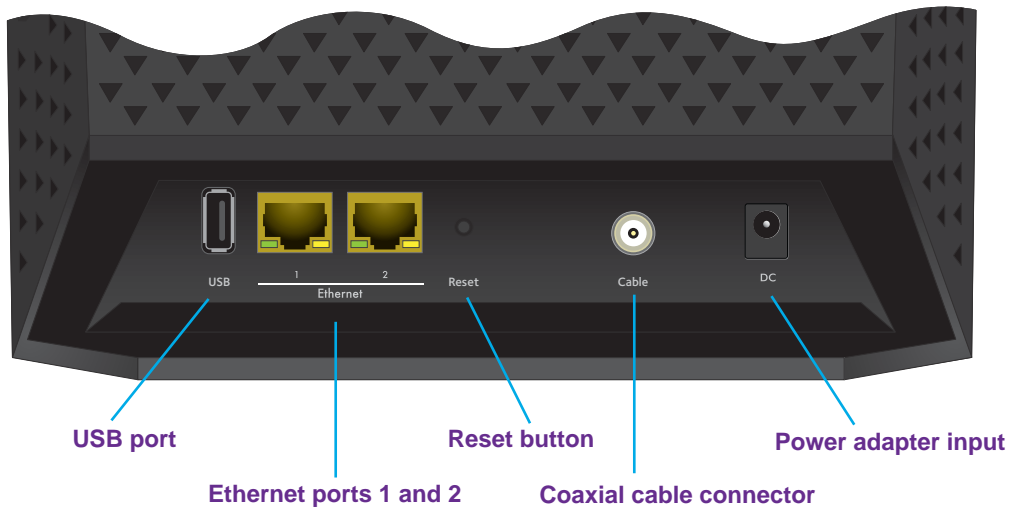


Figure 2. Back panel connections and button

The back panel includes the following components, viewed from left to right:

- **USB port.** One USB 2.0 port lets you connect a USB hard drive, flash drive, or printer to the modem router.
- **Two 10/100/1000 Mbps Ethernet ports.** Use these ports to connect local computers to the Ethernet LAN of the modem router.

Each Ethernet port provides two port LEDs: a left LED (green) and a right port LED (amber), which, together, indicate the operating speed and traffic condition. The following table describes the port LEDs.

Table 3. Ethernet port LED descriptions

LED	Description
LAN port LEDs	<ul style="list-style-type: none"> • Left LED solid green. The port is operating at 1000 Mbps. • Left LED blinking green. The port is transmitting or receiving data while operating at 1000 Mbps. • Right LED solid amber. The port is operating at 100 Mbps or 10 Mbps. • Right LED blinking amber. The port is transmitting or receiving data while operating at 100 Mbps or 10 Mbps. • Both LEDs off. The port is not connected to a powered-on Ethernet device.

- **Recessed Reset button.** To set the modem router to the original factory settings, press and hold the **Reset** button for at least eight seconds. For more information, see [Return the Modem Router to Its Factory Default Settings](#) on page 113.
- **Coaxial cable connector.** Attach a coaxial cable to the cable service provider's connection.
- **Power input connector.** Attach the DC power adapter cable to this input.

Position Your Modem Router

The modem router lets you access your network from 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 modem router. For example, the thickness and number of walls the WiFi signal passes through can limit the range.

For best results, place your modem router according to the following guidelines:

- Place your modem router on an upper floor of a multifloor home or office.
- Place your modem 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 modem router is within reach of an AC power outlet and near Ethernet cables for wired computers.
- Place the modem router in an elevated location, minimizing the number walls and ceilings between the modem router and your other devices.
- Place the modem router away from electrical devices such as these:
 - Ceiling fans
 - Home security systems
 - Microwaves
 - Computers
 - Baby monitors
 - Base of a cordless phone

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

When you use multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is five channels (for example, use Channels 1 and 6, or 6 and 11).

Install and Activate Your Cable Modem

The most common way to cable your modem router is the simplest, without any other routers or gateways on the same network. You can also cable the modem router to another router or gateway and log in to the modem router to specify this setting.

Cable the Modem Router

The modem router comes configured to work as both a modem and a router. You can share your Internet connection without connecting the modem router to a router or gateway.

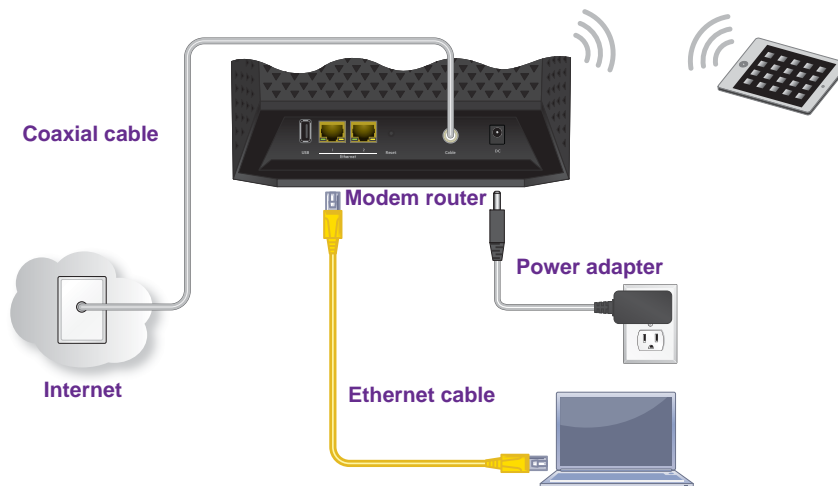


Figure 3. Modem router in a simple network

➤ **To cable your modem router:**

1. Connect a coaxial cable.

Use the coaxial cable that your cable company provides to connect the cable port on the modem router to a cable wall outlet or a line splitter.

Note: For XFINITY cable Internet service, Comcast XFINITY recommends connecting your modem router to a cable wall outlet.

2. Connect the power adapter provided in the package to the modem router and plug the power adapter into an electrical outlet.
3. Press the **Power On/Off** button on the back panel of the modem router.

The Power LED lights green.

4. Wait for the modem router to come online

The modem router comes online when the Internet LED stops blinking and lights solid green.

This process might take up to 10 minutes.

5. Connect a computer or WiFi device to the modem router.

For more information, see *Connect to the Network* on page 21.

You can log in to the modem router to view or change its settings.

Activate Your Internet Service

➤ **To activate your Internet service:**

1. Visit your cable Internet provider's website and follow the onscreen instructions to activate your Internet service.

Cable Internet Provider	Contact Information
Bright House Networks	http://support.brighthouse.com 1-866-898-9101
Cablevision	http://www.cablevision.com https://install.optimum.com/JointInstall/ Telephone number depends on your region. Note: When you attempt to contact Cablevision online, you are directed to the Optimum web page. Optimum is a brand name of Cablevision.

Cable Internet Provider	Contact Information
Comcast XFINITY	http://www.comcast.com/activate http://www.XFINITY.com/internetsetup http://www.XFINITY.com/internetsupport 1-800-XFINITY (1-800-934-6489) For more information, see Activate Your Internet Service with Comcast XFINITY on page 16.
Cox	https://activation.cox.net/selfactivation/start.cox 1-888-556-1193
Mediacom	https://maestro.mediacomcc.com/walledgarden/page/login.jsp 1-844-2SIMPLE (1-844-274-6753)
Time Warner Cable	https://elb02.activatemymodem.com/authentication 1-800-892-2253

Note: Your cable Internet provider's contact information might change. You can also find the contact information in your monthly Internet service billing statement.

2. If you are unable to activate your Internet service using the instructions on your cable Internet provider's website, call your cable Internet provider and do the following:
 - a. When asked, provide your account information and provide the modem router's model number, which is C6250, serial number, and MAC address.

The serial number and MAC address are on the label on the modem router, which is on the bottom of the cable modem.
 - b. Wait for your cable Internet provider to confirm that your modem router is active.
 - c. If you do not get an Internet connection with the modem router, ask your cable Internet provider to look for your modem router online, and do one of the following depending what your cable Internet provider tells you about your modem router:
 - If the modem router is not visible, your cable Internet provider can give you instructions to verify why the modem router does not connect with your high-speed Internet service.
 - If the modem router is visible to your cable Internet provider, reboot the modem router. Check your online status again.

Activate Your Internet Service with Comcast XFINITY

If you use Comcast XFINITY, you can set up Internet service by using Comcast XFINITY's self-activation process. If you are unable to self-activate your modem router, call Comcast XFINITY customer service. After you complete the setup, perform a speed test.

Before you start the self-activation process, make sure that your account number, account phone number, and login information (your email address or user name and password) are nearby.

➤ **To activate your Internet connection with Comcast XFINITY's self-activation process:**

1. Close all web browsers.
2. Launch a web browser.

You are redirected to the XFINITY self-activation page. If you are not redirected to the XFINITY self-activation page, visit www.comcast.com/activate.

3. Provide your XFINITY credentials and complete the self-activation process.
This process might take up to 15 minutes, during which the modem router reboots a couple of times.
4. If you are unable to activate your modem router using the XFINITY self-activation process, call Comcast XFINITY customer service at 1-800-XFINITY (1-800-934-6489).
 - a. When asked, provide your account information and provide the modem router's model number and MAC address, which are on the product label on the modem router.

For more information, see [Product Label](#) on page 23.

- b. Wait for Comcast XFINITY to confirm that your modem router is active.
- c. If you do not get an Internet connection with the modem router, ask Comcast XFINITY to look for your modem router online, and do one of the following depending on what Comcast XFINITY tells you about your modem router:
 - If the modem router is not visible, Comcast XFINITY can give you instructions to verify why the modem router does not connect with your high-speed Internet service.
 - If the modem router is visible to Comcast XFINITY, reboot the modem router. Check your online status again.

Perform a Speed Test

To determine the accurate Internet speed, visit the speed test website of your cable Internet provider and perform a speed test.

If your actual speed is lower than your subscribed speed, contact your cable Internet provider.

Cable the Modem Router to a Router and Use Bridge Mode

In the unlikely situation that you want to use the modem router as a cable modem only that you can connect to an existing router or gateway, you must cable the modem router to the router or gateway, log in to the modem router, and change its router mode setting. Changing this setting prevents certain network conflicts that can occur when two devices on the same network perform routing functions such as network address translation (NAT) and DHCP

(assigning IP addresses to devices on the network). This turns the modem router into a bridged modem.

Note: If the modem router functions as a cable modem only (that is, as a bridged modem or in bridge mode), the modem router's WiFi radios are turned off.

➤ **To cable your modem router to a gateway or router and change the router mode:**

1. Connect a coaxial cable.

Use the coaxial cable that your cable company provides to connect the cable port on the modem router to a cable wall outlet or a line splitter.

2. Connect the power adapter to the modem router and plug the power adapter into an electrical outlet.

The Power LED lights green.

3. On your computer or wireless device, find and select the WiFi network.

The WiFi network name is on the product label.

4. Join the WiFi network and enter the WiFi password.

The password is on the product label.

Your wireless device connects to the WiFi network.

5. Launch an Internet browser.

6. Type **http://www.routerlogin.net**.

A login window opens.

7. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

8. Click the **OK** button.

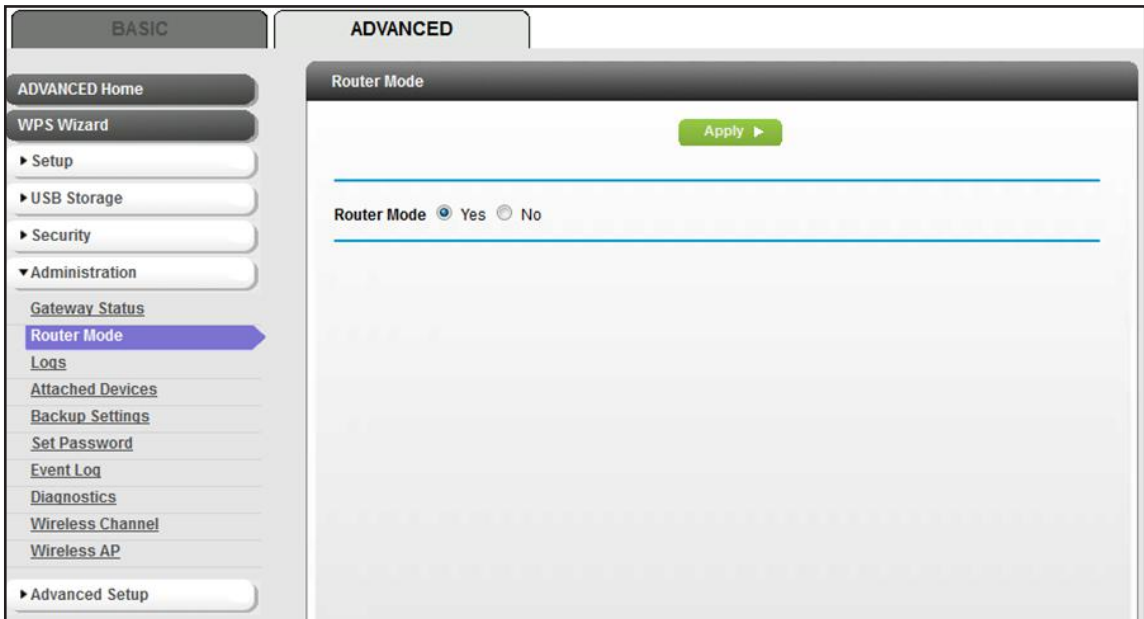
The BASIC Home page displays.

9. Select **ADVANCED > Administration > Router Mode**.

The Router Mode page displays.

10. Select the **No** radio button.

By default, the **Yes** radio button is selected.



With the **No** setting, the modem router works as a bridge and obtains IP information from the cable Internet provider.

11. Click the **Apply** button.

Your settings are saved.

12. Follow the instructions that came with your router or gateway to connect it to the modem router.



CAUTION:

When the modem router is in bridge mode, you must connect *only one* device (your other router) to one of the Ethernet ports on the modem router. In most cases, an Internet service provider (ISP) provides only one public IP address and connecting multiple devices can cause conflicts and can cause your devices to stop working.

2

2 Connect to the Network and Access the Modem Router

This chapter describes how to use NETGEAR genie to connect to the modem router.

This chapter contains the following sections:

- *Connect to the Network*
- *Types of Logins and Access*
- *Product Label*
- *Access NETGEAR genie*
- *Access the Modem Router with the NETGEAR genie App*

Note: For information about installing the modem router, see the *AC1600 WiFi Cable Modem Router Model C6250 Quick Start Guide* that comes in the product package. You can also download this guide from downloadcenter.netgear.com.

Connect to the Network

You can connect to the modem 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 Modem Router Through an Ethernet Cable

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

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

1. Make sure that the modem router is receiving power (its Power LED is lit).
2. Connect an Ethernet cable to an Ethernet port on your computer.
3. Connect the other end of the Ethernet cable to one of the numbered Ethernet LAN ports on the modem router.

Your computer connects to the LAN. A message might display on your computer screen to notify you that an Ethernet cable is connected.

Join the WiFi Network of the Modem Router

Choose either the manual or the WPS method to add a WiFi device such as a computer, iPhone, iPad, or gaming device to the WiFi network of the modem router.

Manual Method

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

1. Make sure that the modem router is receiving power (its Power LED is lit).
2. On the WiFi device that you want to connect to your modem router, open the software application that manages your WiFi connections.

This software scans for all WiFi networks in your area.

3. Look for your network and select it.

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

4. Enter the modem router password.

The default WiFi password (also referred to as passphrase or key) is on the product label.

5. Click the **Connect** button.

The device connects to the WiFi network of the modem router.

Wi-Fi Protected Setup Method

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

➤ **To use WPS to connect a device to the WiFi network of the modem router:**

1. Make sure that the modem router is receiving power (its Power LED is lit).
2. Check the WPS instructions for your computer or wireless device.
3. Press the **WPS** button on the side panel of the modem router for three seconds.
4. Within two minutes, press the **WPS** button on your WiFi device, or follow the WPS instructions that came with the device.

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

For more information, see *Use the WPS Wizard to Add a Device to the WiFi Network* on page 45.

Types of Logins and Access

The modem router supports separate types of logins that serve different purposes. It is important that you understand the difference so that you know which of the following logins to use when:

- **Modem router login.** This login logs you in to the modem router interface from NETGEAR genie. For more information, see *Access NETGEAR genie* on page 23.
- **WiFi network key or password.** Your modem router is preset with a unique WiFi network name (SSID) and password for WiFi access. This information is on the product label (see *Product Label* on page 23). For information about joining the WiFi network, see *Join the WiFi Network of the Modem Router* on page 21.

Note: Your modem router broadcasts dual-band 2.4 GHz and 5 GHz WiFi signals. The label shows the SSID for the 2.4 GHz signal. For information about 5 GHz WiFi settings, see *Manage the Basic WiFi Settings and WiFi Security of the Main Network* on page 36.

Product Label

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

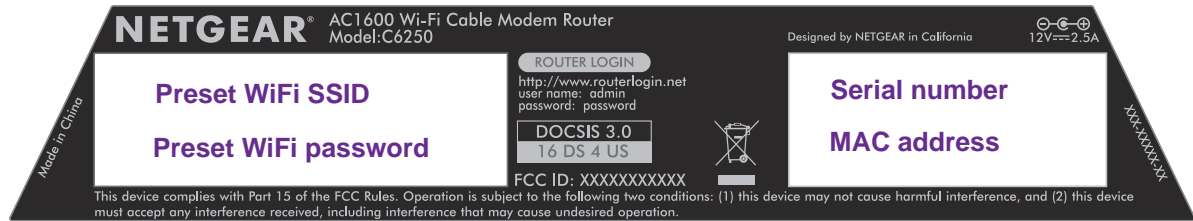


Figure 4. Product label

Access NETGEAR genie

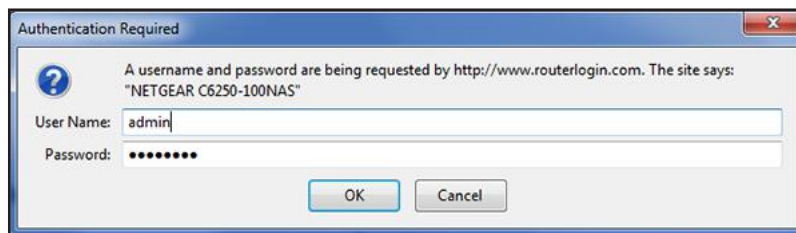
NETGEAR genie runs on any device with a web browser.

The following procedure assumes that you installed the modem router and that your computer or another device is connected with an Ethernet cable or over WiFi with the preset security settings that are listed on the product label.

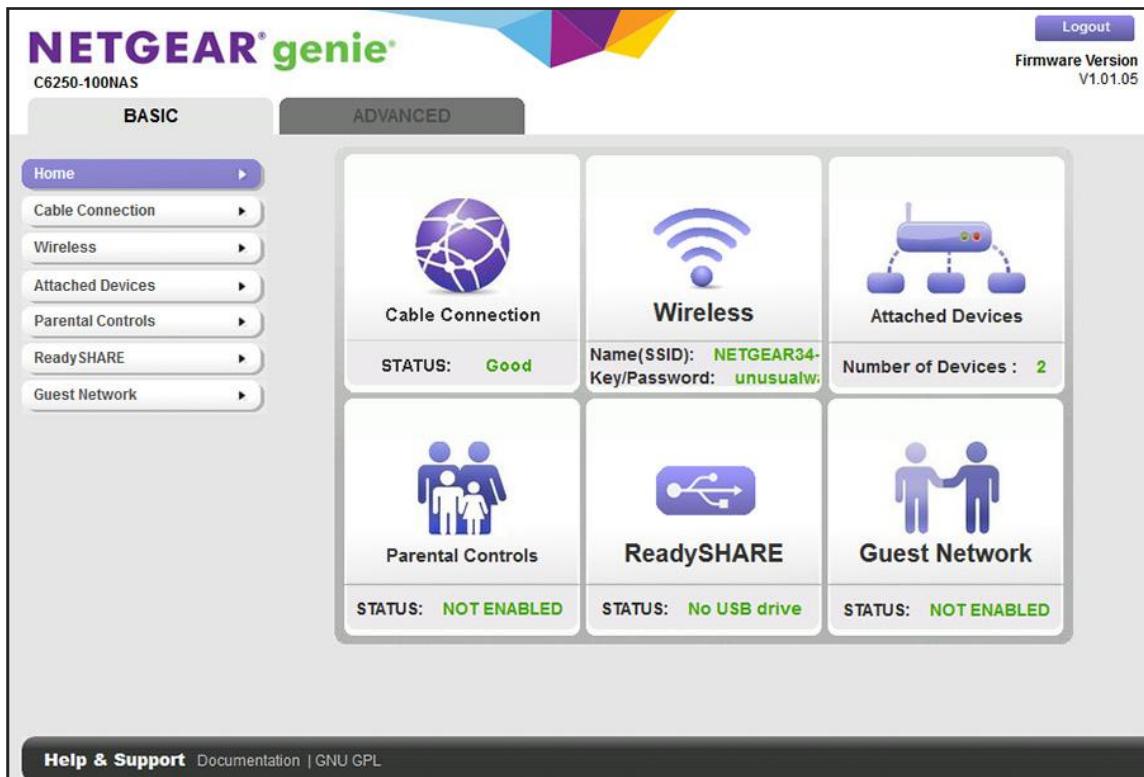
➤ **To access NETGEAR genie to change the settings and monitor your modem router:**

1. Apply power to the modem router.
2. Launch an Internet browser from a computer or WiFi device that is connected to the network.
3. Type **http://www.routerlogin.net**.

Note: You can also type **http://www.routerlogin.com**, or **http://192.168.0.1**.
This manual uses **http://www.routerlogin.net**.



4. Type **admin** for the user name and **password** for the password.
5. Click the **OK** button.




The modem router BASIC Home page provides a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the sections of the dashboard to view more detailed information. The left column provides the menus, and at the top is the **ADVANCED** tab that you can use to access more menus and pages.

If you cannot log in to the modem router or your browser does not display the NETGEAR genie page, check the following:

- Make sure that the computer is connected to one of the two Ethernet LAN ports or over WiFi to the modem router.
- Make sure that your browser does not cache the previous page by closing and reopening the browser.
- If your computer is set to a static or fixed IP address (this type of setting is uncommon), change the setting to obtain an IP address automatically from the modem router (see [View or Manually Set Up the IPv4 Internet Settings](#) on page 30).

For more troubleshooting information, see [You Cannot Log In to the Modem Router](#) on page 186.

Access the Modem Router with the NETGEAR genie App

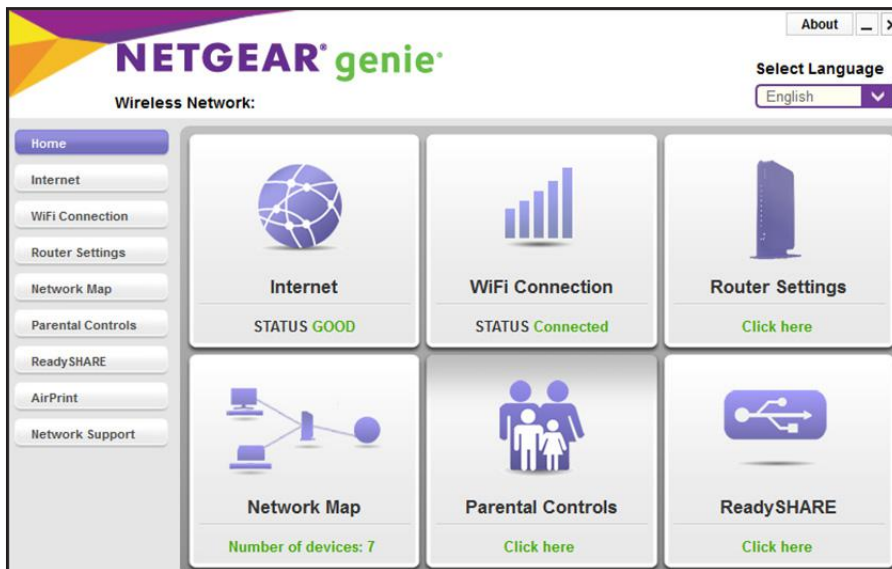
The genie app  is the easy dashboard for managing, monitoring, and repairing your home network from a smartphone, tablet, or computer. The genie app can help you with the following:

- Automatically repair common WiFi network problems.
- Easily manage modem router features such as Live Parental Controls, guest access, speed test, and more.
- Share and stream music or videos.

➤ **To use the genie app to access the modem router:**

1. Visit the NETGEAR genie web page at netgear.com/genie.
2. Follow the onscreen instructions to install the app on your smartphone, tablet, or computer.
3. Launch the genie app.

The genie app dashboard page displays. The following figure shows the genie app dashboard for a Windows computer.



Customize the Internet Settings

3

This chapter describes how to customize your Internet settings. For information about setting up your Internet connection with your cable service provider, see the following sections:

The chapter contains the following sections:

- *View the Cable Initialization of the Modem Router*
- *Change the Cable Connection Starting Frequency*
- *View or Manually Set Up the IPv4 Internet Settings*
- *Manage the MTU Size*

View the Cable Initialization of the Modem Router

You can track the cable initialization procedure of the modem router and get details about the downstream and upstream cable channels. The time is displayed after the modem router is initialized.

The modem router automatically goes through the following steps in the provisioning process:

1. Scans and locks the downstream frequency and then ranges the upstream channels.
2. Obtains a WAN IP address for the modem router.
3. Connects to the Internet.



WARNING:

Do not change the starting frequency unless your cable service provider instructs you to do so. Changing the starting frequency incorrectly causes serious connection and Internet problems. If you must change the starting frequency, see [Change the Cable Connection Starting Frequency](#) on page 28.

➤ **To view the status of the modem router initialization:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **Cable Connection**.

The screenshot shows the 'Cable Connection' settings page. The 'Starting Frequency' field is set to 0. The 'Startup Procedure' table shows the following data:

Procedure	Status	Comment
Acquire Downstream Channel	651000000 Hz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Security	Enabled	BPI+
IP Provisioning Mode	Honor MDD	honorMdd(4)

The 'Downstream Bonded Channels' table shows the following data:

Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1	Locked	QAM256	16	651000000 Hz	2.3 dBmV	40 dB	0	0
2	Locked	QAM256	1	561000000 Hz	1.9 dBmV	40.1 dB	0	0
3	Locked	QAM256	2	567000000 Hz	1.8 dBmV	40.1 dB	0	0
4	Locked	QAM256	3	573000000 Hz	2.1 dBmV	40.2 dB	0	0
5	Locked	QAM256	4	579000000 Hz	2.3 dBmV	40.2 dB	0	0
6	Locked	QAM256	5	585000000 Hz	2.5 dBmV	40.2 dB	0	0
7	Locked	QAM256	6	591000000 Hz	2.7 dBmV	40.2 dB	0	0
8	Locked	QAM256	7	597000000 Hz	2.9 dBmV	40.2 dB	0	0

The Startup Procedure section displays the initialization progress.

6. Scroll down to see the rest of the Downstream Bonded Channels section, the Upstream Bonded Channels section, and the current system time.

The Downstream Bonded Channel and Upstream Bonded Channels sections display the status of each channel and details about each channel.

Change the Cable Connection Starting Frequency

The starting frequency for the cable connection is automatically generated. For most Internet connections, you do not need to change this information.



WARNING:

Do not change the starting frequency unless your cable Internet provider instructs you to do so. Changing the starting frequency incorrectly causes serious connection and Internet problems.

- To change the starting frequency:
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type <http://www.routerlogin.net>.

A login window opens.

- Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
- Click the **OK** button.
The BASIC Home page displays.
- Select **Cable Connection**.

Cable Connection

Apply X Cancel

Frequency start Value
This field below allows you to modify the frequency the cable modem start with its scan during initialization and registration. Enter the new start frequency and restart the cable modem for it to take effect.

Starting Frequency 0

Startup Procedure

Procedure	Status	Comment
Acquire Downstream Channel	651000000 Hz	Locked
Connectivity State	OK	Operational
Boot State	OK	Operational
Security	Enabled	BPI+
IP Provisioning Mode	Honor MDD	honorMdd(4)

Downstream Bonded Channels

Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Correctables	Uncorrectables
1	Locked	QAM256	16	651000000 Hz	2.3 dBmV	40 dB	0	0
2	Locked	QAM256	1	561000000 Hz	1.9 dBmV	40.1 dB	0	0
3	Locked	QAM256	2	567000000 Hz	1.8 dBmV	40.1 dB	0	0
4	Locked	QAM256	3	573000000 Hz	2.1 dBmV	40.2 dB	0	0
5	Locked	QAM256	4	579000000 Hz	2.3 dBmV	40.2 dB	0	0
6	Locked	QAM256	5	585000000 Hz	2.5 dBmV	40.2 dB	0	0
7	Locked	QAM256	6	591000000 Hz	2.7 dBmV	40.2 dB	0	0
8	Locked	QAM256	7	597000000 Hz	2.9 dBmV	40.2 dB	0	0

- In the **Starting Frequency** field, type a number as instructed by your cable Internet provider.



WARNING:

Do not change the starting frequency unless your cable Internet provider instructs you to do so. Changing the starting frequency incorrectly causes serious connection and Internet problems.

- Click the **Apply** button.

Your settings are saved. The scanning process starts and the modem router comes online after approximately three minutes.

View or Manually Set Up the IPv4 Internet Settings

In general, the modem router receives the Internet settings dynamically from the cable service provider. However, you can view or change the Internet settings.

The main Internet settings that you can configure are the IP address of the modem router (dynamic or static) and the Domain Name System (DNS) server (dynamic or static).

➤ To view or change the Internet settings:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > Internet Setup**.

The screenshot shows the 'Internet Setup' page in the 'ADVANCED' tab. The left sidebar contains a navigation menu with 'Internet Setup' highlighted. The main content area has the following sections:

- Account Name (If Required):** C6250-100NAS
- Domain Name (If Required):** [Empty field]
- Internet IP Address:**
 - Get Dynamically from ISP
 - Use Static IP Address
 - IP Address: [0] . [0] . [0] . [0]
 - IP Subnet Mask: [0] . [0] . [0] . [0]
 - Gateway IP Address: [0] . [0] . [0] . [0]
- Domain Name Server (DNS) Address:**
 - Get Automatically from ISP
 - Use These DNS Servers
 - Primary DNS: [] . [] . [] . []
 - Secondary DNS: [] . [] . [] . []
 - Tertiary DNS: [] . [] . [] . []

6. View or change the settings for the IP address and DNS server.

The default settings usually work fine. If problems occur with the connection, check the settings that your cable service provider gave you.

The following table describes the fields on the Internet Setup page.

Field	Description
Account Name (If Required)	Enter the account name provided by your cable service provider. This name might also be called the host name. If you do not know or did not receive an account name, leave the default name, which is the model number of the modem router.
Domain Name (If Required)	Enter the domain name provided by your cable service provider. If you do not know the domain name, leave this field blank.
Internet IP Address	
Get Dynamically from ISP	Your cable service provider uses DHCP to assign your IP address. Your cable service provider automatically assigns these addresses.
Use Static IP Address	Enter the IP address, IP subnet mask, and gateway IP address that your cable service provider assigned to you. The gateway is the provider gateway to which your modem router connects.
Domain Name Server (DNS) Address	
The DNS server is used to look up site addresses based on their names.	
Get Dynamically from ISP	Your cable service provider uses DHCP to assign your DNS servers. Your cable service provider automatically assigns this address.
Use These DNS Servers	If you know that your cable service provider does not automatically transmit DNS addresses to the modem router during login, select this option, and enter the IP address of your cable service provider primary DNS server. If secondary and tertiary DNS server addresses are available, enter these also.

- If you changed the settings, click the **Apply** button.

Your settings are saved.

Manage the MTU Size

The maximum transmission unit (MTU) is the largest data packet that 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 MTU setting than the other devices, the data packets must be split or “fragmented” to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often the default value. In some situations, changing the value fixes one problem but causes another.

Leave the MTU unchanged unless one of these situations occurs:

- You experience problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
 - A secure website that does not open or displays only part of a web page
 - Yahoo email
 - MSN portal
 - America Online’s DSL service
- You use VPN and experience severe performance problems.
- You used a program to optimize MTU for performance reasons and now you are experiencing connectivity or performance problems.

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

Table 4. 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 modem 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.
1460	Usable by AOL if you do not send or receive large email attachments, for example.

Table 4. Common MTU sizes (continued)

MTU	Application
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.

Change the MTU Size



WARNING:

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

➤ **To change the MTU size:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > WAN Setup**.
The WAN Setup page displays.
6. In the **MTU Size** field, enter a value from 256 to 1500.
The default value is 1500.
7. Click the **Apply** button.
Your settings are saved.

Manage the Basic WiFi Network Settings

4

This chapter describes how to configure the basic settings for the main WiFi network and guest WiFi network and how to use the WPS wizard.

This chapter contains the following sections:

- *Manage the Basic WiFi Settings and WiFi Security of the Main Network*
- *Use the WPS Wizard to Add a Device to the WiFi Network*
- *Manage the Basic WiFi Settings and WiFi Security of the Guest Network*

Note: For information about the managing the advanced WiFi settings, see *Chapter 11, Manage the Advanced WiFi Network Settings*.

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

The modem router comes with preset security. This means that the WiFi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. The preset SSID and password are uniquely generated for every device to protect and maximize your WiFi security. You can find the preset SSID and password on the product label (see *Product Label* on page 23).

IMPORTANT:

NETGEAR recommends that you do *not* change your preset security settings. If you decide to change your preset security settings, make a note of the new settings and store the note in a safe place where you can easily find it.

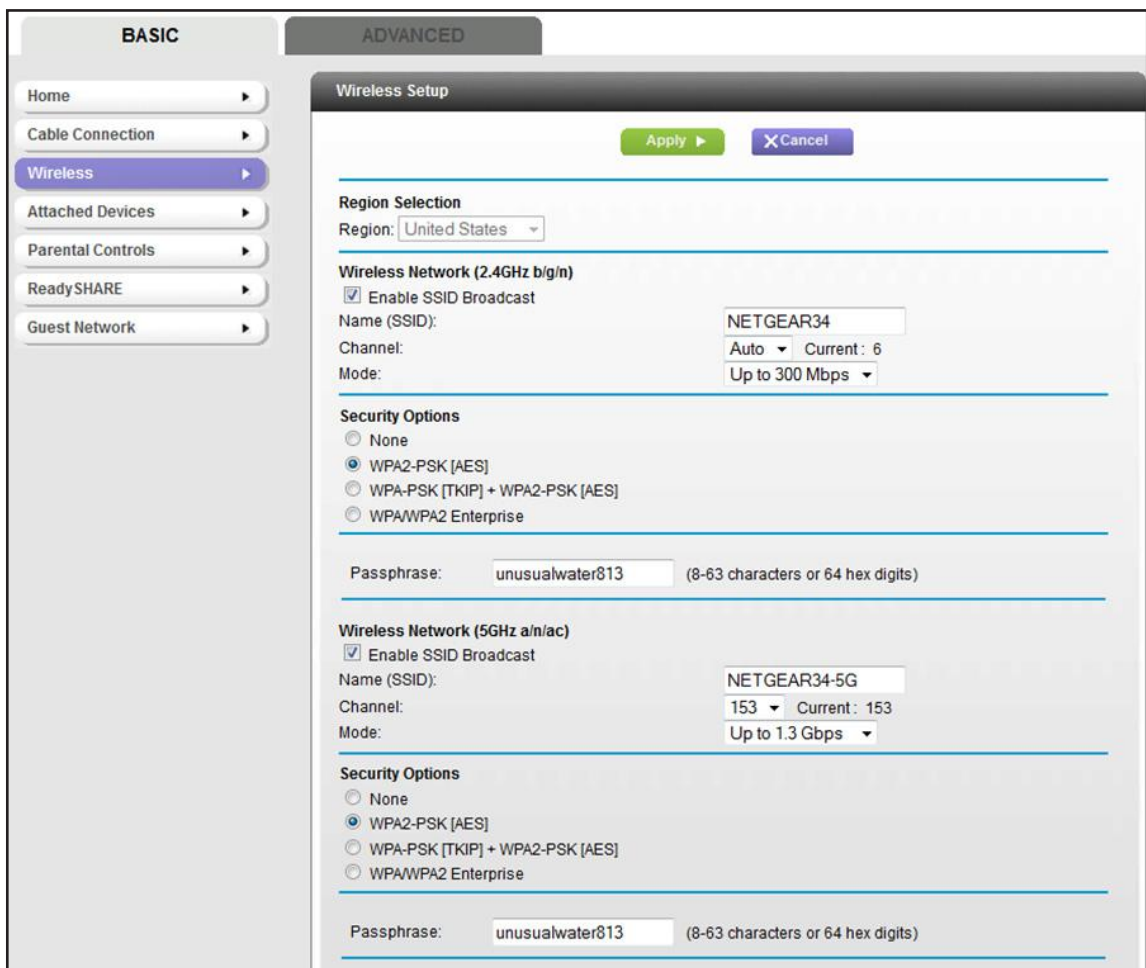
View or Change the Basic WiFi Settings

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

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

➤ To view or change basic WiFi settings for main WiFi network:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **BASIC > Wireless**.



6. View or change the basic WiFi settings and security settings.

The following table describes the fields on the Wireless Setup page.

Field	Description
Region Selection	
Region	The selection from the Region menu is fixed at United States and the menu is masked out.
Wireless Network (2.4GHz b/g/n)	
Enable SSID Broadcast	By default, the modem router broadcasts its SSID so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast, clear the Enable SSID Broadcast check box. Turning off the SSID broadcast provides additional WiFi security, but users must know the SSID to be able to join the WiFi network of the modem router.

AC1600 WiFi Cable Modem Router

Field	Description
Name (SSID)	<p>The SSID is the WiFi network name. If you did not change the SSID, the default SSID displays. The default SSID is also printed on the product label (see <i>Product Label</i> on page 23).</p> <p>Note: NETGEAR recommends that you do not change the default SSID. If you must change the SSID, enter a 32-character (maximum), case-sensitive name in this field.</p>
Channel	<p>From the Channel menu, select Auto for automatic channel selection or select an individual channel. The default selection is Auto and the channel that is in use is stated next to the menu.</p> <p>Note: Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this situation occurs, experiment with different channels to see which one is the best.</p> <p>Note: If you use multiple WiFi access points (APs), reduce interference by selecting different channels for adjacent APs. NETGEAR recommends a channel spacing of four channels between adjacent APs (for example, use Channels 1 and 5, or 6 and 10).</p>
Mode	<p>From the Mode menu, select one of the following modes:</p> <ul style="list-style-type: none">• Up to 54 Mbps. Legacy mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11n devices to functioning at up to 54 Mbps.• Up to 145 Mbps. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network but limits 802.11n devices to functioning at up to 145 Mbps. This mode is the default mode.• Up to 300 Mbps. Performance mode. This mode allows 802.11n, 802.11g, and 802.11b devices to join the network and allows 802.11n devices to function at up to 300 Mbps. <p>Note: WEP and WPA-PSK security support speeds of up to 54 Mbps. Even if your devices are capable of a higher speed, WEP and WPA-PSK security limit their speed to 54 Mbps.</p>

Field	Description
Security Options	
This information applies to the 2.4 GHz WiFi network.	
<p>Note: NETGEAR recommends that you do <i>not</i> change your preset security settings (WPA2-PSK [AES]).</p> <p>If you must change the WiFi security, select one of the following WiFi security options for the modem router's WiFi network:</p> <ul style="list-style-type: none"> • None. An open WiFi network that does not provide any security. Any WiFi device can join the network. NETGEAR recommends that you do <i>not</i> use an open WiFi network. • WEP. Wired Equivalent Privacy (WEP) security is a legacy authentication and data encryption mode that is superseded by WPA-PSK and WPA2-PSK. The WEP option displays only if you select Up to 54 Mbps from the Mode menu. For information about configuring WEP, see Configure WEP Legacy WiFi Security for the Main WiFi Network on page 43. • WPA-PSK [TKIP]. WPA provides a secure connection but is superseded by WPA2. The WPA-PSK [TKIP] option displays only if you select Up to 54 Mbps from the Mode menu. To use this type of security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the modem router's WiFi network, a user must enter this passphrase. • WPA2-PSK [AES]. This type of security is the default setting and enables WiFi devices that support WPA2 to join the modem router's 2.4 GHz WiFi network. If you did not change the passphrase, the default passphrase displays. The default passphrase is printed on the product label (see Product Label on page 23). 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. NETGEAR recommends that you do not change the default passphrase. If you must change the passphrase, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the modem router's WiFi network, a user must enter this passphrase. • WPA-PSK [TKIP] + WPA2-PSK [AES]. This type of security enables WiFi devices that support either WPA or WPA2 to join the modem router's 2.4 GHz WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps. To use this type of security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the modem router's WiFi network, a user must enter this passphrase. • WPA/WPA2 Enterprise. This type of security requires that your WiFi network can access a RADIUS server. For information about configuring WPA/WPA2 Enterprise, see Configure WPA/WPA2 Enterprise WiFi Security on page 41. 	
Wireless Network (5GHz 11a/n/ac)	
Enable SSID Broadcast	By default, the modem router broadcasts its SSID so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast, clear the Enable SSID Broadcast check box. Turning off the SSID broadcast provides additional WiFi security, but users must know the SSID to be able to join the WiFi network of the modem router.
Name (SSID)	The SSID is the WiFi network name. If you did not change the SSID, the default SSID displays. The default SSID is also printed on the product label (see Product Label on page 23). Note: NETGEAR recommends that you do not change the default SSID. If you must change the SSID, enter a 32-character (maximum), case-sensitive name in this field.

Field	Description
Channel	<p>From the Channel menu, select an individual channel. The default selection is 153.</p> <p>Note: Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this situation occurs, experiment with different channels to see which one is the best.</p> <p>Note: If you use multiple WiFi access points (APs), reduce interference by selecting different channels for adjacent APs. NETGEAR recommends a channel spacing of four channels between adjacent APs.</p>
Mode	<p>From the Mode menu, select one of the following modes:</p> <ul style="list-style-type: none"> • Up to 289 Mbps. Legacy mode. This mode allows 802.11ac, 802.11na, and 802.11a devices to join the network but limits 802.11ac and 802.11na devices to functioning at up to 289 Mbps. • Up to 600 Mbps. Neighbor-friendly mode for reduced interference with neighboring WiFi networks. This mode allows 802.11ac, 802.11na, and 802.11a devices to join the network, allows 802.11na devices to function at up to 600 Mbps, and limits 802.11ac devices to functioning at up to 600 Mbps. • Up to 1.3 Gbps. Performance mode. This mode allows 802.11ac, 802.11na, and 802.11a devices to join the network and allows 802.11ac devices to function at up to 1300 Mbps. This mode is the default mode.
<p>Security Options This information applies to the 5 GHz WiFi network.</p> <p>Note: NETGEAR recommends that you do <i>not</i> change your preset security settings (WPA2-PSK [AES]).</p> <p>If you must change the WiFi security, select one of the following WiFi security options for the modem router's WiFi network:</p> <ul style="list-style-type: none"> • None. An open WiFi network that does not provide any security. Any WiFi device can join the network. NETGEAR recommends that you do <i>not</i> use an open WiFi network. • WPA2-PSK [AES]. This type of security is the default setting and enables WiFi devices that support WPA2 to join the modem router's 2.4 GHz WiFi network. If you did not change the passphrase, the default passphrase displays. The default passphrase is printed on the product label (see Product Label on page 23). 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. NETGEAR recommends that you do not change the default passphrase. If you must change the passphrase, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the modem router's WiFi network, a user must enter this passphrase. • WPA-PSK [TKIP] + WPA2-PSK [AES]. This type of security enables WiFi devices that support either WPA or WPA2 to join the modem router's 2.4 GHz WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps. To use this type of security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the modem router's WiFi network, a user must enter this passphrase. • WPA/WPA2 Enterprise. This type of security requires that your WiFi network can access a RADIUS server. For information about configuring WPA/WPA2 Enterprise, see Configure WPA/WPA2 Enterprise WiFi Security on page 41. 	

7. If you changed the settings, click the **Apply** button.

Your settings are saved.

8. Set up and test your WiFi devices and computers to make sure that they can connect over WiFi.

If they do not, check the following:

- Is your WiFi device connected to your network or another WiFi network in your area? Some WiFi devices automatically connect to the first open network (without WiFi security) that they discover.
- Does your WiFi device display as a connected device in the web management interface? (See *View Devices Currently on the Network* on page 104.) If it does, it is connected to the network.
- Do you use the correct network name (SSID) and password? The default SSID and default password are on the product label.

Configure WPA/WPA2 Enterprise WiFi Security

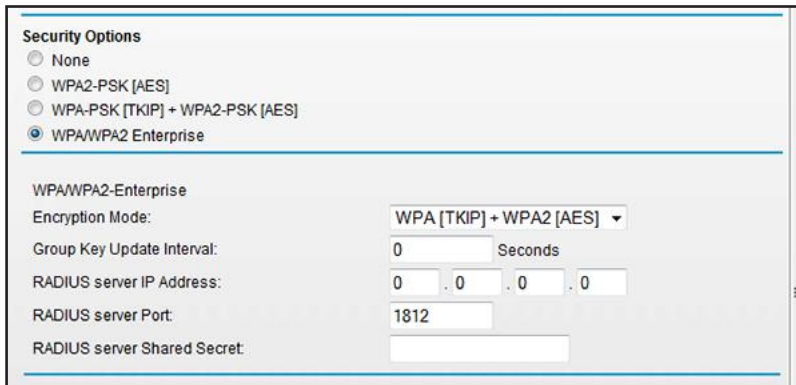
Remote Authentication Dial In User Service (RADIUS) is an enterprise-level method for centralized Authentication, Authorization, and Accounting (AAA) management. To provide WPA/WPA2 enterprise WiFi security, the WiFi network that the modem router provides must be able to access a RADIUS server.

Note: WPS and WPA/WPA2 enterprise security cannot function together. When you enable WPA/WPA2 enterprise security, WPS is disabled.

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

➤ To configure WPA/WPA2 enterprise security:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **Wireless**.
The Wireless Setup page displays.
6. In the Security Options section, select the **WPA/WPA2 Enterprise** radio button.



7. In the Security Options (WPA/WPA2 Enterprise) section, enter the settings as described in the following table.

Field	Description
Encryption Mode	From the Encryption Mode menu, select the enterprise mode: <ul style="list-style-type: none"> • 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. • WPA [TKIP] +WPA2 [AES]. This type of security enables WiFi devices that support either WPA or WPA2 to join the modem router's WiFi network.
Group Key Update Interval	Enter the interval in seconds after which the RADIUS group key is updated.
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 modem 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 modem router and the RADIUS server during authentication of a WiFi user.

8. Click the **Apply** button.
Your settings are saved.
9. Make sure that you can reconnect over WiFi to the network with its new security settings.
If you cannot connect over WiFi, check the following:
- If your computer or WiFi device is already connected to another WiFi network in your area, disconnect it from that WiFi network and connect it to the WiFi network that the modem router provides. Some WiFi devices automatically connect to the first open network without WiFi security that they discover.
 - If your computer or WiFi device is trying to connect to your network with its old settings (before you changed the settings), update the WiFi network selection in your computer or WiFi device to match the current settings for your network.

- Does your WiFi device display as an attached device? (See [View Devices Currently on the Network](#) on page 104.) If it does, it is connected to the network.
- Are you using the correct network name (SSID) and password?

Configure WEP Legacy WiFi Security for the Main WiFi Network

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 modem router is capable of speeds of up to 300 Mbps).

Note: WPS and WEP security cannot function together. When you enable WEP security, WPS is disabled.

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

➤ **To configure WEP security for the main WiFi network:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **BASIC > Wireless**.
The Wireless Setup page displays.
6. From the **Mode** menu, select **Up to 54 Mbps**.
The WEP and WPA-PSK [TKIP] security options become visible.
7. In the Security Options section, select the **WEP** radio button.

8. From the **Authentication Type** menu in the Security Encryption (WEP) section, select one of the following types:
 - **Shared Key**. Clients can use only Shared Key authentication.
 - **Automatic**. Clients can use either Open System or Shared Key authentication.
9. From the **Encryption Strength** menu in the Security Encryption (WEP) section, select the encryption key size:
 - **64-bit**. Standard WEP encryption, using 40/64-bit encryption.
 - **128-bit**. Standard WEP encryption, using 104/128-bit encryption. This selection provides stronger encryption security.
10. In the Security Encryption (WEP) Key section, generate the key automatically:
 - a. In the **Passphrase** field, enter a passphrase.
 - b. Click the **Generate** button.

For 64-bit WEP, four different WEP keys are generated and the four key fields are populated with different WEP keys. For 128-bit WEP, only one WEP key is generated and the four key fields are populated with the same WEP key.
 - c. 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 main WiFi network, a user must enter the key value for the key that you specified as the active key.
11. Click the **Apply** button.

Your settings are saved.

Use the WPS Wizard to Add a Device to the WiFi Network

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

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

WPS supports WPA and WPA2 WiFi security. If your modem router network is open (no WiFi security is set, which is not the default setting for the modem router), connecting with WPS automatically sets WPA + WPA2 WiFi security on the modem router network and generates a random passphrase. You can view this passphrase (see *Manage the Basic WiFi Settings and WiFi Security of the Main Network* on page 36).

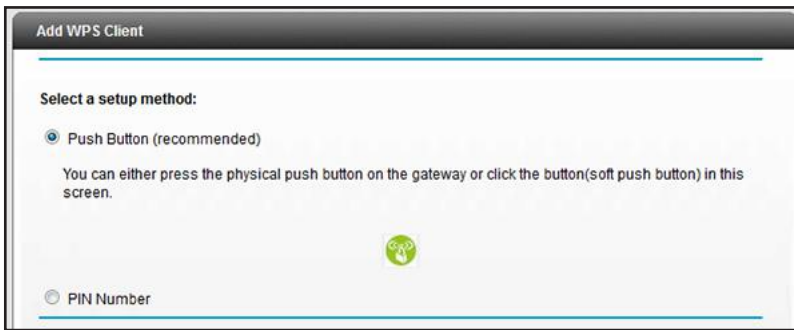
Use WPS with the Push Button Method

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


- **To let a WiFi device join the modem router's main WiFi network using WPS with the push button method:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > WPS Wizard**.



6. Click the **Next** button.



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

7. Either click the  button onscreen or press the **WPS** button on the right side panel of the modem router for three seconds.

For two minutes, the modem router attempts to find the WiFi device (that is, the client) that you want to join the modem router's main WiFi network.

During this time, both WiFi LEDs on the front panel of the modem router blink amber.

8. Within two minutes, go to the WiFi device and press its **WPS** button to join the modem router's main WiFi network without entering a password.

After the modem router establishes a WPS connection, the LED lights solid green and the Add WPS Client page displays a confirmation message.

9. To verify that the WiFi device is connected to the modem router's main WiFi network, select **BASIC > Attached Devices**.

The WiFi device displays onscreen.

Use WPS with the PIN Method

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

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

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.

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

A login window opens.

3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

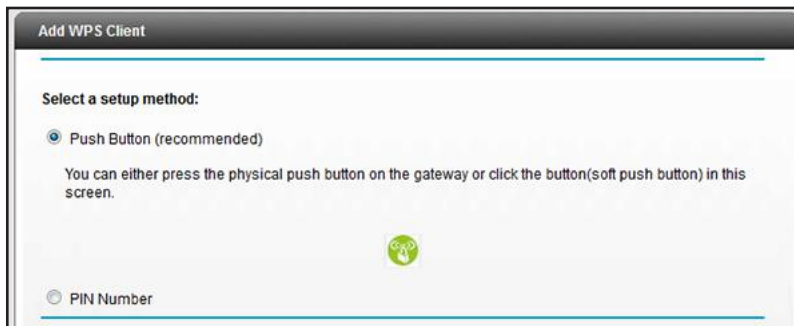
4. Click the **OK** button.

The BASIC Home page displays.

5. Select **ADVANCED > WPS Wizard**.



6. Click the **Next** button.



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

7. Select the **PIN Number** radio button.



8. In the **Enter Client's PIN** field, enter the PIN number of the WiFi device.
9. Click the **Next** button.

For four minutes, the modem router attempts to find the WiFi device (that is, the client) that you want to join the modem router's main WiFi network.

During this time, both WiFi LEDs on the front panel of the modem router blink amber.

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

When the modem router establishes a WPS connection, the LED lights solid green and the Add WPS Client page displays a confirmation message.

11. To verify that the WiFi device is connected to the modem router's main WiFi network, select **BASIC > Attached Devices**.

The WiFi device displays onscreen.

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

A guest network allows visitors to use the Internet without using your WiFi security key. By default, the guest WiFi network is disabled. You can enable and configure the guest WiFi network for each WiFi band: 2.4 GHz b/g/n and 5.0 GHz a/n/ac.

Set Up and Enable a Guest Network

The WiFi mode of the guest WiFi network depends on the WiFi mode of the main WiFi network. For example, if you configure the WiFi mode for the main WiFi network as Up to 54 Mbps in the 2.4 GHz band, the guest WiFi network also functions in the Up to 54 Mbps mode in the 2.4 GHz band. For information about configuring the WiFi mode, see [Manage the Basic WiFi Settings and WiFi Security of the Main Network](#) on page 36.

➤ **To enable and configure the settings for the guest WiFi network:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **BASIC > Guest Network**.

6. Enable the guest network and configure its WiFi settings.

The following table describes the fields on the Guest Network Settings page.

Field	Description
Wireless Network (2.4GHz b/g/n) - Profile	
Enable Guest Network	By default, the guest WiFi network is disabled. To enable the guest WiFi network for the 2.4 GHz WiFi band, select the Enable Guest Network check box.
Enable SSID Broadcast	By default, the modem router broadcasts its SSID of the 2.4 GHz WiFi band so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast for the 2.4 GHz WiFi band for the guest WiFi network, clear the Enable SSID Broadcast check box.
Allow guests to see each other and access my local network	By default, WiFi clients that are connected to the 2.4 GHz WiFi band of the guest WiFi network cannot access WiFi devices or Ethernet devices that are connected to the main WiFi network. To allow access to the main WiFi network, select the Allow guests to see each other and access my local network check box.
Guest Wireless Network Name (SSID)	The SSID is the 2.4 GHz WiFi band name. If you did not change the SSID, the default SSID displays, which is NETGEAR-Guest. If you want to change the SSID in the 2.4 GHz WiFi band for the guest WiFi network, enter a 32-character (maximum), case-sensitive name in this field.
Security Options - Profile	
<p>If you want to change the WiFi security, select one of the following WiFi security options for the 2.4 GHz band of the guest WiFi network:</p> <ul style="list-style-type: none"> • None. An open WiFi network that does not provide any security. Any WiFi device can join the 2.4 GHz band of the guest WiFi network. This is the default setting for the guest WiFi network. • WEP. Wired Equivalent Privacy (WEP) security is a legacy authentication and data encryption mode that is superseded by WPA-PSK and WPA2-PSK. The WEP option displays only if you configure the WiFi mode for the main WiFi network as Up to 54 Mbps in the 2.4 GHz band (see Manage the Basic WiFi Settings and WiFi Security of the Main Network on page 36). For information about configuring WEP, see Configure WEP Legacy WiFi Security for the Guest WiFi Network on page 52. • WPA-PSK [TKIP]. WPA provides a secure connection but is superseded by WPA2. The WPA-PSK [TKIP] option displays only if you configure the WiFi mode for the main WiFi network as Up to 54 Mbps in the 2.4 GHz band (see Manage the Basic WiFi Settings and WiFi Security of the Main Network on page 36). To use this type of security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the modem router's WiFi network, a user must enter this passphrase. • 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 to allow 802.11n devices to connect to the 2.4 GHz band of the guest WiFi network at the fastest speed. If your network includes older devices that do not support WPA2, select WPA-PSK [TKIP] + WPA2-PSK [AES] security. To use WPA2 security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the 2.4 GHz band of the guest WiFi network, a user must enter this passphrase. • WPA-PSK [TKIP] + WPA2-PSK [AES]. This type of security enables WiFi devices that support either WPA or WPA2 to join the 2.4 GHz band of the guest WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps. To use WPA + WPA2 security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the 2.4 GHz band of the guest WiFi network, a user must enter this passphrase. 	

Field	Description
Wireless Network (5GHz a/n/ac) - Profile	
Enable Guest Network	By default, the guest WiFi network is disabled. To enable the guest WiFi network for the 5 GHz WiFi band, select the Enable Guest Network check box.
Enable SSID Broadcast	By default, the modem router broadcasts its SSID of the 5 GHz WiFi band so that WiFi stations can detect the WiFi name (SSID) in their scanned network lists. To turn off the SSID broadcast for the 5 GHz WiFi band for the guest WiFi network, clear the Enable SSID Broadcast check box.
Allow guests to see each other and access my local network	By default, WiFi clients that are connected to the 5 GHz WiFi band of the guest WiFi network cannot access WiFi devices or Ethernet devices that are connected to the main WiFi network. To allow access to the main WiFi network, select the Allow guests to see each other and access my local network check box.
Guest Wireless Network Name (SSID)	The SSID is the 5 GHz WiFi band name. If you did not change the SSID, the default SSID displays, which is NETGEAR-5G-Guest. If you want to change the SSID in the 5 GHz WiFi band for the guest WiFi network, enter a 32-character (maximum), case-sensitive name in this field.
Security Options - Profile	
<p>If you want to change the WiFi security, select one of the following WiFi security options for the 5 GHz band of the guest WiFi network:</p> <ul style="list-style-type: none"> • None. An open WiFi network that does not provide any security. Any WiFi device can join the 5 GHz band of the guest WiFi network. This is the default setting for the guest WiFi network. • WPA2-PSK [AES]. WPA2 provides a secure and fast connection but some older WiFi devices do not detect WPA2 and support only WPA. Select WPA2 to allow 802.11n devices to connect to the 5 GHz band of the guest WiFi network at the fastest speed. If your network includes older devices that do not support WPA2, select WPA-PSK [TKIP] + WPA2-PSK [AES] security. To use WPA2 security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the 5 GHz band of the guest WiFi network, a user must enter this passphrase. • WPA-PSK [TKIP] + WPA2-PSK [AES]. This type of security enables WiFi devices that support either WPA or WPA2 to join the 5 GHz band of the guest WiFi network. However, WPA-PSK [TKIP] is less secure than WPA2-PSK [AES] and limits the speed of WiFi devices to 54 Mbps. To use WPA + WPA2 security, in the Passphrase field, enter a phrase of 8 to 63 characters. To join the 5 GHz band of the guest WiFi network, a user must enter this passphrase. 	

7. If you changed the settings, click the **Apply** button.

Your settings are saved.

8. Make sure that you can reconnect over WiFi to the guest network. If you cannot connect over WiFi, check the following:
 - Is your WiFi device connected to your network or another WiFi network in your area? Some WiFi devices automatically connect to the first open network (without WiFi security) that they discover.
 - Does your WiFi device display as a connected device in the web management interface? (See [View Devices Currently on the Network](#) on page 104.) If it does, it is connected to the network.
 - Do you use the correct network name (SSID) and password?

Configure WEP Legacy WiFi Security for the Guest WiFi Network

Wired Equivalent Privacy (WEP) security is a legacy authentication and data encryption mode that is superseded by WPA-PSK and WPA2-PSK. WEP supports speeds of up to 54 Mbps (the modem router is capable of speeds of up to 300 Mbps).

IMPORTANT:

The WiFi mode of the guest WiFi network depends on the WiFi mode of the main WiFi network. For you to be able to configure WEP in the guest WiFi network, first configure the mode for the main WiFi network as Up to 54 Mbps. For information about configuring the WiFi mode, see *Manage the Basic WiFi Settings and WiFi Security of the Main Network* on page 36.

- To configure WEP security for the guest WiFi network:
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **BASIC > Guest Network**.
The Guest Network Settings page displays.
 6. In the Security Options section, select the **WEP** radio button.

These options display only if you select the **Up to 54 Mbps** mode for the *main* WiFi network.

Security Options - Profile

None
 WEP
 WPA-PSK [TKIP]
 WPA2-PSK [AES]
 WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Encryption (WEP)

Authentication Type: Automatic ▾

Encryption Strength: 64-bit ▾

Security Encryption (WEP) Key

Passphrase:

Key 1: 0000000000

Key 2: 0000000000

Key 3: 0000000000

Key 4: 0000000000

7. From the **Authentication Type** menu in the Security Encryption (WEP) section, select one of the following types:
 - **Shared Key.** Clients can use only Shared Key authentication.
 - **Automatic.** Clients can use either Open System or Shared Key authentication.
8. From the **Encryption Strength** menu in the Security Encryption (WEP) section, select the encryption key size:
 - **64-bit.** Standard WEP encryption, using 40/64-bit encryption.
 - **128-bit.** Standard WEP encryption, using 104/128-bit encryption. This selection provides stronger encryption security.
9. In the Security Encryption (WEP) Key section, generate the key automatically:
 - a. In the **Passphrase** field, enter a passphrase.
 - b. Click the **Generate** button.

For 64-bit WEP, four different WEP keys are generated and the four key fields are populated with different WEP keys. For 128-bit WEP, only one WEP key is generated and the four key fields are populated with the same WEP key.
 - c. 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 guest WiFi network, a user must enter the key value for the key that you specified as the active key.
10. Click the **Apply** button.

Your settings are saved.

Secure Your Network

5

This chapter describes how to use the firewall features of the modem router to prevent objectionable content from reaching the computers and other devices connected to your network and how to control which computers and devices are allowed access to the network.

This chapter includes the following sections:

- *Set Up Parental Controls*
- *Allow or Block Access to Your Network*
- *Block Keywords and Domains for HTTP Traffic*
- *Block Access to Services and Applications*
- *Schedule When Security Features Are Active*
- *Set Up Security Event Email Notification*

For information about more advanced ways to configure Internet security, see *Chapter 12, Manage Port Forwarding and Port Triggering*.

Set Up Parental Controls

The first time that you select **Parental Controls** from the BASIC Home page, your browser goes to the *Parental Controls* website, where you can learn more about Parental Controls. To set up Parental Controls, you must download the genie app.



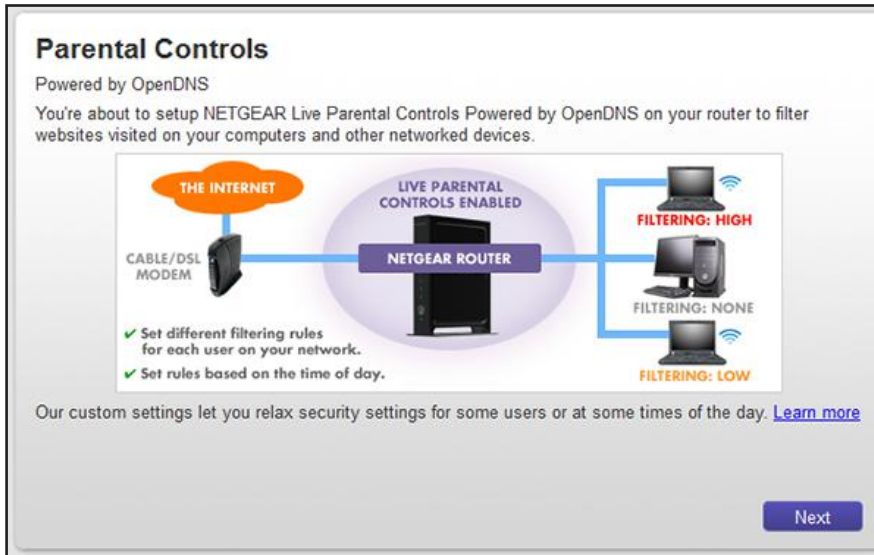
Figure 5. Parental Controls website

➤ To set up Parental Controls:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **Parental Controls**.
The *Parental Controls* website opens.
6. Click the button for the genie app or version that you want to download and use.
7. Follow the onscreen instructions to download and install the genie app.

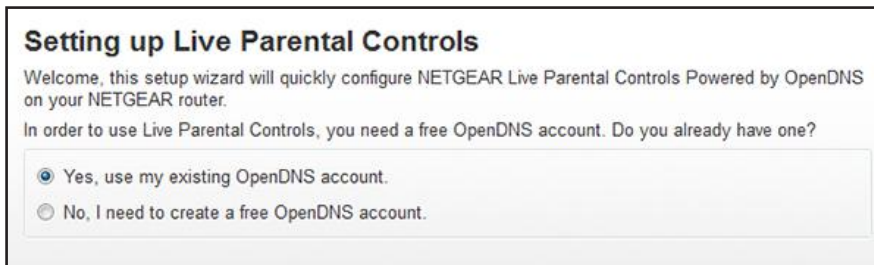
8. Open the genie app and select **Parental Controls**.

Live Parental Controls automatically starts.



9. Click the **Next** button, read the note, and click the **Next** button again.

Because Live Parental Controls uses free OpenDNS accounts, you are prompted to log in or create a free account.



10. Select a radio button as follows:

- If you already own an OpenDNS account, leave the **Yes** radio button selected.
- If you did not yet create an OpenDNS account, select the **No** radio button.

If you are creating an account, the following page displays.

Create a free OpenDNS account
Please enter your information below.

Username

Password

Confirm Password

Email

Confirm Email

- a. Complete the fields.
- b. Click the **Next** button.

After you log on or create your account, the filtering level page displays.

Live Parental Controls: choose a filtering level for your network
All computers connected to your router will be protected from the content you select below. You can customize your Live Parental Controls later on our website.

None
Nothing blocked.

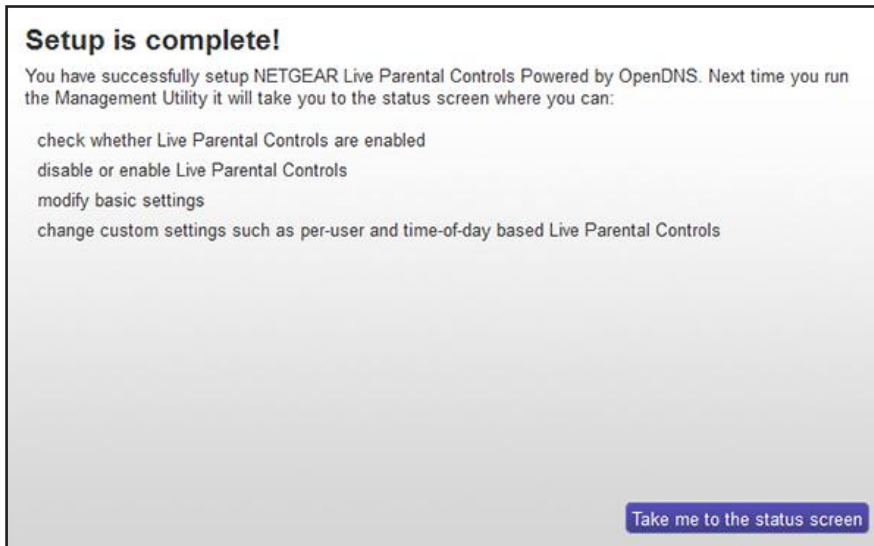
Minimal
Protects only against phishing attacks.

Low
Protects against pornography and phishing attacks.

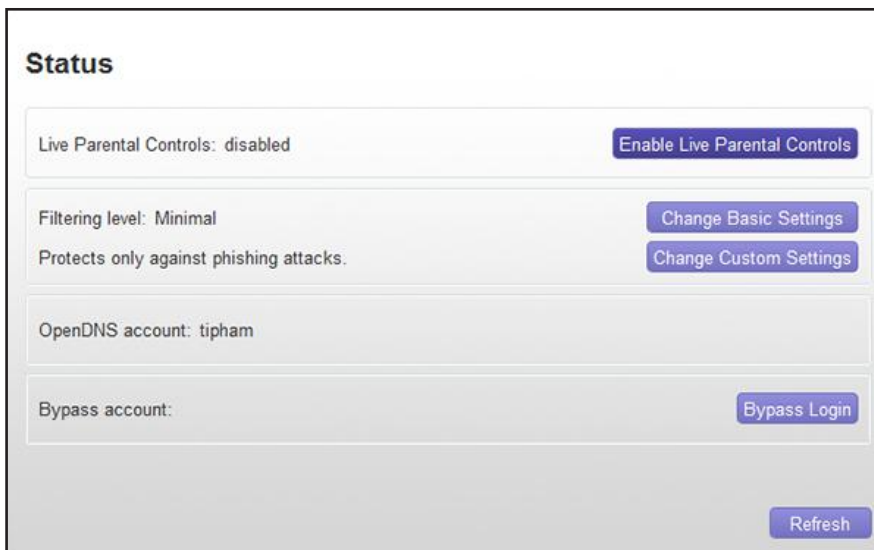
Moderate
Protects against all adult-related sites, illegal activity and phishing attacks.

High

11. Select a radio button for a filtering level and click the **Next** button.



12. Click the **Take me to the status screen** button.



Parental Controls are now set up for the modem router.

13. To enable Parental Controls, click the **Enable Live Parental Controls** button.

Allow or Block Access to Your Network

You can use access control to block or allow access of devices to your network. You define access by selecting or specifying the MAC addresses of the wired and WiFi devices that can either access your entire network or are blocked from accessing your entire network.

Enable and Manage Network Access Control

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

➤ **To set up network access control:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Access Control**.

The screenshot shows the 'Access Control' configuration page. The 'Turn on Access Control' checkbox is checked. The 'Access Rule' section has 'Allow all new devices to connect' selected. Below this is a table of allowed devices:

Status	Device Name	IP Address	MAC Address	Connection Type
Allowed	BusinessLaptop	192.168.0.11	60:66:66:da:66:7c	Wireless
Allowed	Pavilion	192.168.0.12	d0:df:9a:9d:9b:41	Wireless

Below the table, there are links to view lists of allowed and blocked devices not currently connected to the network.

6. 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 the device is in the list of blocked devices.

7. Click the **Apply** button.

Your settings are saved.

8. Select an access rule for new devices:

- **Allow all new devices to connect.** With this setting, if you add a new device, it can access your network. You do not need to enter its MAC address on this page. NETGEAR recommends that you leave this radio button selected.
- **Block all new devices from connecting.** With this setting, if you add a new device, before it can access your network, you must enter its MAC address for an Ethernet connection and its MAC address for a WiFi connection in the allowed list. For more information, see *Manage Network Access Control Lists* on page 60.

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.

9. To manage access for currently connected computers and devices, do one of the following:

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

		Allow	Block	Edit	Refresh
<input type="checkbox"/>	Status	Device Name	IP Address	MAC Address	Connection Type
<input type="checkbox"/>	Allowed	BusinessLaptop	192.168.0.11	60:66:66:da:66:7c	Wireless
<input type="checkbox"/>	Blocked	Pavilion	192.168.0.12	d0:df:9a:9d:9b:41	Wireless

10. Click the **Apply** button.

Your settings are saved.

Manage Network Access Control Lists

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

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

Each network device owns a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F (uppercase or lowercase) only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the WiFi card or network interface device. If you cannot see the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses through the web management interface of the modem router (see *View Devices Currently on the Network* on page 104).

Add Disconnected Devices to or Remove Them from the Allowed List

If you set up an access list that blocks all new devices from accessing your network, you can specify which devices that are currently not connected to the modem router but that were connected in the past are allowed to access your network when they attempt to reconnect.

Note: You cannot remove a device from the allowed list while the device is currently connected to the modem router. To remove such a device, you must wait until the device disconnects from the modem router.

- **To add a disconnected device to the allowed list or remove it from the allowed list:**
1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > Security > Access Control**.
The Access Control page displays.
 6. Click the **View list of allowed devices not currently connected to the network** link.

The screenshot shows the 'Access Control' page in the router's web interface. The 'Access Control' section is active, and the 'Allow all new devices to connect' option is selected. The 'Allowed' table contains one entry: BusinessLaptop (192.168.0.11, 60:66:66:da:66:7c, Wireless). The 'View list of allowed devices not currently connected to the network' section contains one entry: Unknown (d0:df:9a:9d:9b:41, Wireless). The 'View list of blocked devices not currently connected to the network' section is empty.

A table displays the detected device names, MAC addresses, and connection types of the devices that are not connected but allowed to access the network.

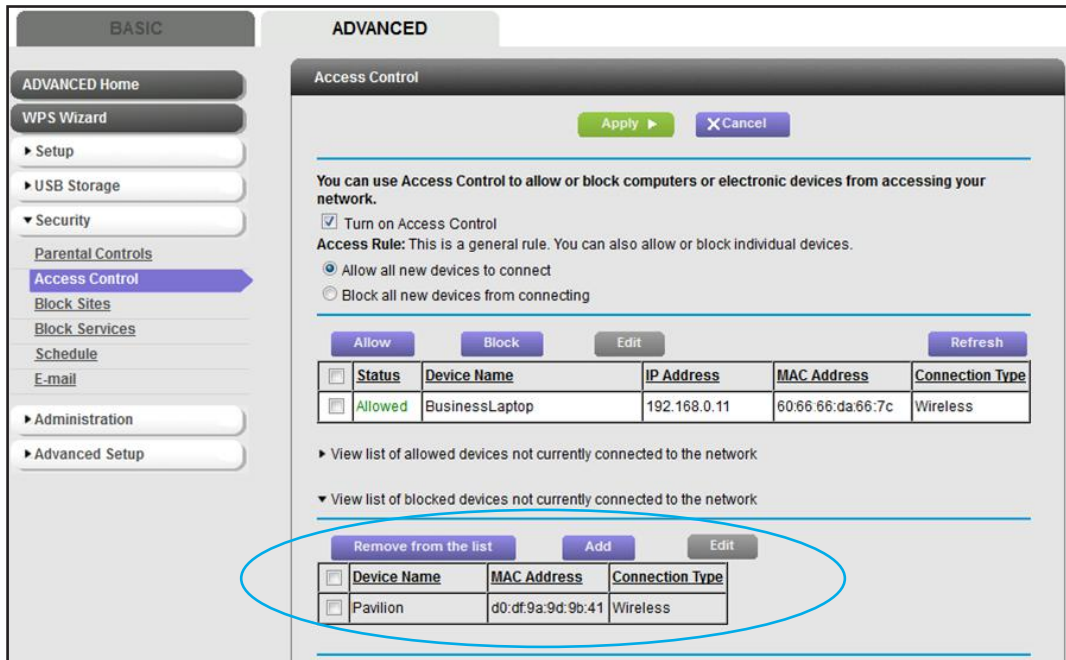
7. To add a device to the allowed list, do the following:
 - a. Click the **Add** button.
The Add Allowed Device page displays.
 - b. Enter the MAC address and device name for the device that you want to allow.
 - c. Click the **Add** button on the Add Allowed Device page.
The device is added to the allowed list on the Access Control page.
8. To remove a device from the allowed list, do the following:
 - a. Select the check box for the device.
 - b. Click the **Remove from the list** button.
The device is removed from the allowed list.
9. Click the **Apply** button.
Your settings are saved.

Add Disconnected Devices to or Remove Them from the Blocked List

If you set up an access list that allows all new devices from accessing your network, you can specify which devices that are currently not connected to the modem router but that were connected in the past are blocked from accessing your network when they attempt to reconnect.

Note: You cannot remove a device from the blocked list after you just placed it on the blocked list and the device is still connected to the modem router. (In such a situation, the device would be blocked from accessing your network when it attempts to reconnect.) To remove such a device, you must wait until the device disconnects from the modem router.

- **To add a disconnected device to the blocked list or remove it from the blocked list:**
1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > Security > Access Control**.
The Access Control page displays.
 6. Click the **View list of blocked devices not currently connected to the network** link.



A table displays the detected device names, MAC addresses, and connection types of the devices that are not connected and blocked from accessing the network.

7. To add a device to the blocked list, do the following:

- a. Click the **Add** button.

The Add Blocked Device page displays.

- b. Enter the MAC address and device name for the device that you want to block.
c. Click the **Add** button on the Add Blocked Device page.

The device is added to the blocked list on the Access Control page.

8. To remove a device from blocked list, do the following:

- a. Select the check box for the device.
b. Click the **Remove from the list** button.

The device is removed from the blocked list.

9. Click the **Apply** button.

Your settings are saved.

Change the Permission for a Device or Change the Device Name on a List

For a device on the blocked list, whether or not currently connected to the network, you can change the permission and move the device to the allowed list. Similarly, for a device on the allowed list, whether or not currently connected to the network, you can change the permission and move the device to the blocked list. For a device on any access list, you can change the device name that displays in the list. You cannot change the MAC address of a device on an access list.

➤ **To change the permission or device name for a device on an access list:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Access Control**.
The Access Control page displays.
6. Select a device on an access control list:
 - To select a device that is currently connected to the modem router, select its associated check box in the table.

<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	
Allow		Block		Edit		Refresh	
<input type="checkbox"/>	Status	Device Name	IP Address	MAC Address	Connection Type		
<input type="checkbox"/>	Allowed	BusinessLaptop	192.168.0.11	60:66:66:da:66:7c	Wireless		
<input type="checkbox"/>	Blocked	Pavilion	192.168.0.12	d0:df:9a:9d9b:41	Wireless		

- To select a device that is not connected to the modem router and that is on the allowed list, do the following:
 - a. Click the **View list of allowed devices not currently connected to the network** link.
 - b. Select its associated check box in the table (that is, the allowed list).
- To select a device that is not connected to the modem router and that is on the blocked list, do the following:
 - a. Click the **View list of blocked devices not currently connected to the network** link.
 - b. Select its associated check box in the table (that is, the blocked list).

The **Edit** button that is associated with the table becomes available.

7. Click the **Edit** button.
The Edit Device Name page displays.
8. To change the permission, from the **Access Control** menu, select either **Allow** or **Block**.
9. To change the device name, enter a new name in the **Device Name** field.
10. Click the **Apply** button.
Your settings are saved and the Access Control page displays again.

Block Keywords and Domains for HTTP Traffic

You can block keywords and domain names (website names) to prevent HTTP traffic between your network and websites that include such keywords and names. By default, keyword blocking is disabled and no domains are blocked.

Set Up Blocking

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

➤ **To set up keyword and domain blocking:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Block Sites**.

The screenshot shows the 'Block Sites' configuration page in the router's web interface. The left sidebar contains navigation options: ADVANCED Home, WPS Wizard, Setup, USB Storage, Security, Parental Controls, Access Control, Block Sites (highlighted), Block Services, Schedule, E-mail, Administration, and Advanced Setup. The main content area is titled 'Block Sites' and includes an 'Apply' button and a 'Cancel' button. Below these is a link to learn more about advanced content filtering. The 'Keyword Blocking' section has three radio buttons: 'Never' (selected), 'Per Schedule' (with a dropdown arrow), and 'Always'. Below this is a text input field labeled 'Type Keyword Or Domain Name Here.' with an '+ Add Keyword' button. A list box titled 'Block sites containing these keywords or domain names:' is currently empty. At the bottom, there is a checkbox for 'Allow Trusted IP Address to Visit Blocked Sites' and a 'Trusted IP Address' field with the value '192 . 168 . 0 . 0'.

6. Specify a keyword blocking option:
 - **Per Schedule.** Use keyword blocking according to a schedule that you set and select a schedule from the menu.
For more information, see *Schedule When Security Features Are Active* on page 75.
 - **Always.** Use keyword blocking continuously.
7. In the **Type keyword or domain name here** field, enter a keyword or domain.
Here are some sample entries:
 - Specify XXX to block `http://www.badstuff.com/xxx.html`.
 - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
 - Enter a period (.) to block all Internet browsing access.
8. Click the **Add Keyword** button.
The keyword or domain is added to the **Block sites containing these keywords or domain names** field (which is also referred to as the blocked list).
9. To add more keywords or domains, repeat *Step 7* and *Step 8*.
The keyword list supports up to 32 entries.
10. Click the **Apply** button.
Your settings are saved.

Remove a Keyword or Domain from the Blocked List

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

- **To remove a keyword or domain from the blocked list:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type `http://www.routerlogin.net`.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > Security > Block Sites**.
The Block Sites page displays.
 6. In the **Block sites containing these keywords or domain names** field, select the keyword or domain that you want to remove.
 7. Click the **Delete Keyword** button.

The keyword or domain is removed from the blocked list.

8. Click the **Apply** button.

Your settings are saved.

Remove All Keywords and Domains from the Blocked List

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

➤ To remove all keywords and domains from the blocked list:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Block Sites**.
The Block Sites page displays.
6. Click the **Clear List** button.
All keywords and domains are removed from the blocked list.
7. Click the **Apply** button.
Your settings are saved.

Specify a Trusted Computer

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

➤ To specify a trusted device:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

The BASIC Home page displays.

5. Select **ADVANCED > Security > Block Sites**.

6. Scroll down and select the **Allow trusted IP address to visit blocked sites** check box.
7. In the **Trusted IP Address** field, enter the IP address of the trusted device.

The first three octets of the IP address are automatically populated and depend on the IP address that is assigned to the modem router on the LAN Setup page.

8. Click the **Apply** button.

Your settings are saved.

Block Access to Services and Applications

Services are functions that servers perform at the request of client devices. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about the moves of the players.

When a device on the Internet sends a request for service to a server, the requested service is identified by a service or port number. (For this reason, service blocking is also referred to as port filtering.) The service or port number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with the destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at ietf.org) and published in *RFC1700, Assigned Numbers*. Service numbers for other applications are typically chosen from the range 1024–65535 by the authors of the application. Although the modem router already holds a list of many service port numbers, you are not limited to these choices.

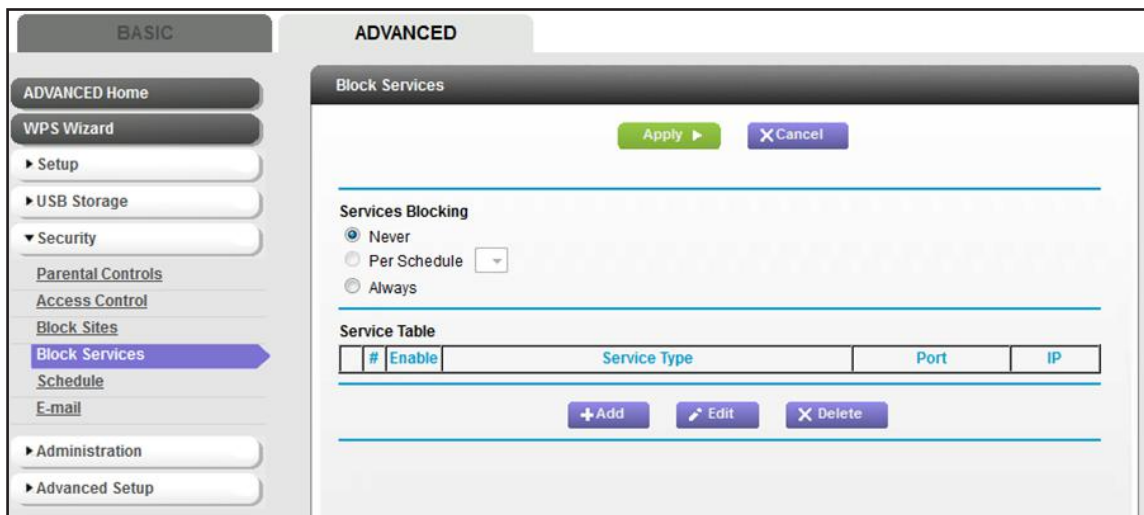
You can block access to specific Internet services by devices on your network. This feature is called service blocking or port filtering. The modem router provides default (predefined) services that you can select to block. You can also add a new service for blocking, but you first must find out which port number or range of numbers the application uses. You can find port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching the Internet.

Block a Default Service

You can set up blocking of specific services to occur continuously or according to a schedule.

➤ To block a default service:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type <http://www.routerlogin.net>.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Block Services**.



6. Specify a keyword blocking option:
 - **Per Schedule.** Use service blocking according to a schedule that you set and select a schedule from the menu.
For more information, see [Schedule When Security Features Are Active](#) on page 75.
 - **Always.** Use service blocking continuously.
7. Click the **Add** button.

8. From the **Service Type** menu, select the default application or service to block.
The menu displays several common services, but you are not limited to these choices. For information about how to add any additional services or applications, see [Add and Block a Custom Service](#) on page 72.
9. Under Filter Services For, select an IP address configuration:
 - **Only This IP Address.** Complete the IP address for the device for which the application or service must be blocked.
 - **IP Address Range.** Complete the IP address range for the devices for which the application or service must be blocked.
 - **All IP Addresses.** The application or service is blocked for all IP addresses on your network.
10. Click the **Add** button.
Your settings are saved in the table on the Block Services page. However, if you restart the modem router, the changes are lost. You must also apply the changes on the Block Services page.
11. On the Block Services page, click the **Apply** button.
Your settings are saved.

Add and Block a Custom Service

If the service that you want to block is not on the default service list, you can define a custom service.

➤ **To add and block a custom service:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Block Services**.



6. Specify a keyword blocking option:
 - **Per Schedule.** Use service blocking according to a schedule that you set and select a schedule from the menu.
For more information, see [Schedule When Security Features Are Active](#) on page 75.
 - **Always.** Use service blocking continuously.
7. Click the **Add** button.

8. From the **Service Type** menu, select **User Defined**.
9. Configure the settings for the custom service or application:
 - **Protocol**. Select a protocol. If you are not sure what protocol the service or application uses, select **TCP/UDP**.
 - **Starting Port** and **Ending Port**. Enter the starting and ending port numbers. If the service or application uses a single port number, enter that number in both fields.
 - **Service Type/User Defined**. Enter a name for the service or application.
10. Under Filter Services For, select an IP address configuration:
 - **Only This IP Address**. Complete the IP address for the device for which the application or service must be blocked.
 - **IP Address Range**. Complete the IP address range for the devices for which the application or service must be blocked.
 - **All IP Addresses**. The application or service is blocked for all IP addresses on your network.
11. Click the **Add** button.

Your settings are saved in the table on the Block Services page. However, if you restart the modem router, the changes are lost. You must also apply the changes on the Block Services page.

12. On the Block Services page, click the **Apply** button.

Your settings are saved.

Change the Settings for a Blocked Service

You can change the settings for a specific service that is being blocked.

➤ **To change the settings for a service:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Block Services**.
The Block Services page displays.
6. Select the radio button next to the service or application that you want to change.
7. Click the **Edit** button.
The Block Services Setup page displays.
8. Change the settings for the service or application.
For information about the settings, see *Add and Block a Custom Service* on page 72.
9. Click the **Add** button.
Your settings are saved in the table on the Block Services page. However, if you restart the modem router, the changes are lost. You must also apply the changes on the Block Services page.
10. To enable or disable blocking of the service, select or clear the **Enable** check box.
11. On the Block Services page, click the **Apply** button.
Your settings are saved.

Remove a Blocked Service

If you no longer need a service on the blocked list, you can remove the service.

➤ **To remove a service:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.

3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Block Services**.
The Block Services page displays.
6. Select the radio button next to the service or application that you want to remove from the table.
7. Click the **Delete** button.
The service or application is removed from the table. A default service or application is not removed from the **Service Type** menu on the Block Services Setup page. However, a custom service or application that you added *is* deleted. If you want to use the same custom service or application again, you must redefine it (see [Add and Block a Custom Service](#) on page 72).
8. Click the **Apply** button.
Your settings are saved.

Schedule When Security Features Are Active

You can specify the days and time that you want a security feature to be active. You can set up multiple schedules, for example, one for each feature, or you can use the same schedule for a combination of different features.

You can apply schedules to the following features:

- Keyword blocking (see [Block Keywords and Domains for HTTP Traffic](#) on page 66)
- Service blocking (see [Block Access to Services and Applications](#) on page 69)

By default, no schedules are set and you can either enable or disable these features.

Set Up a Schedule

The modem router does not provide a default schedule but you can add up to 19 custom schedules.

➤ To set up a schedule:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Schedule**.
The Schedule page displays. The current time is displayed onscreen.
6. Click the **Add** button.

7. In the **Schedule Name** field, enter a name for the schedule.
For example, if you are setting up a schedule for keyword blocking during business hours, you could enter a name that lets you easily identify such a schedule.
8. Set up the schedule for blocking:
 - **Days to Block.** Select the check box for each day that you want to block access or specify that blocking occurs on every day by selecting the **Every Day** check box.
 - **Time of Day to Block.** Select a start and end time for blocking in 24-hour format or select the **All Day** check box for 24-hour blocking.

The start time must be earlier than the end time. For example, you cannot block overnight by specifying 20:00 in the start field and 07:00 in the end field. In such a situation, you must set up two schedules.
9. Click the **Apply** button.
Your settings are saved and the schedule is added to the Schedule Table.

Change a Schedule

You can change the settings for a schedule.

➤ **To change the settings for a schedule:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Schedule**.
The Schedule page displays.
6. Select the radio button next to the schedule that you want to change.
7. Click the **Edit** button.
The Schedule page adjusts.
8. Change the settings for the schedule.
9. Click the **Apply** button.
Your settings are saved and the schedule is updated in the Schedule Table.
10. To display the Schedule Table, click the **Cancel** button.

Remove a Schedule

If you no longer need a schedule, you can remove it.

➤ **To remove a schedule:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > Schedule**.

The Schedule page displays.

6. Select the radio button next to the schedule that you want to remove.
7. Click the **Delete** button.

The schedule is removed from the Schedule Table.

Set Up Security Event Email Notification

To receive logs and alerts by email about websites that users accessed, attempts to access blocked sites, modem router operation, DoS attacks and port scans, WiFi access, and other information, provide your email information on the E-mail page, and specify how often you want to receive logs and alerts.

➤ To set up email notifications:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Security > E-mail**.

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

7. In the **Your Outgoing Mail Server** field, enter the name of your cable service provider's outgoing (SMTP) mail server (such as mail.myISP.com).

You might be able to find this information on the configuration page of your email program or by contacting your cable service provider. If you leave this field blank, log and alert messages are not sent.

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

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

9. If your outgoing email server requires authentication, set up the authentication:
 - a. Select the **My Mail Server requires authentication** check box.
 - b. Complete the **User Name** and **Password** fields for the outgoing email server.
10. If you want alerts to be sent immediately, select the **Send Alerts Immediately** check box.

Email alerts are sent immediately when someone attempts to visit a blocked site.

11. To set up a schedule for logs to be sent, specify the following settings:
 - a. Select an option from the **Send logs according to this schedule** menu:
 - **When log is full**
 - **Hourly**
 - **Daily**
 - **Weekly**
 - **None**
 - b. If you select **Daily** or **Weekly**, select the time from the **Day** menu and select the **a.m.** or **p.m.** radio button.
 - c. If you select **Weekly**, also select the day from the **Day** menu.

Logs are sent automatically. If the log fills before the specified time, the log is emailed. After the log is sent, the log is cleared from the memory of the modem router. If the modem router cannot email the log file, the log buffer might fill. In this case, the modem router overwrites the log and discards its contents.

12. Click the **Apply** button.

Your settings are saved.

Manage the WAN and LAN Network Settings

6

This chapter describes how to manage the WAN and LAN settings.

This chapter contains the following sections:

- *Manage the WAN Security Settings*
- *Set Up a Default DMZ Server*
- *Manage the SIP Application-Level Gateway*
- *Manage the Modem Router's LAN IP Address Settings*
- *Manage IP Address Reservation*
- *Manage the IPv6 LAN Settings*
- *Change the Modem Router's Device Name*
- *Manage the Built-In DHCP Server*
- *Manage the DHCP Server Address Pool*
- *Manage Universal Plug and Play*

For information about managing the MTU size, see *Manage the MTU Size* on page 32.

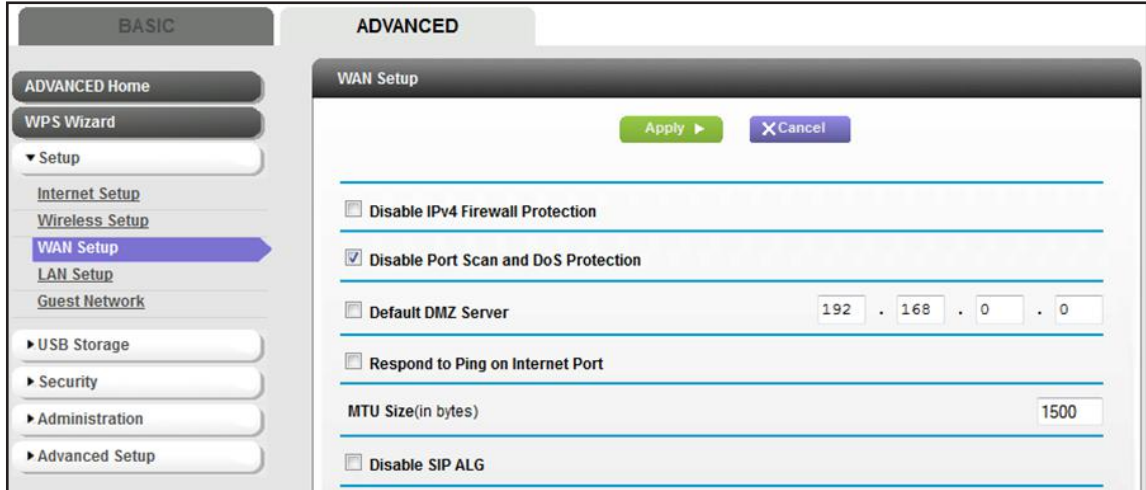
Manage the WAN Security Settings

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

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

➤ **To change the default WAN security settings:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > WAN Setup**.



6. View or change the security settings.

7. The following table describes the protection and ping options on the WAN Setup page.

Field	Description
Disable IPv4 Firewall Protection	IPv4 firewall protection can secure your network against malicious packets. To disable IPv4 firewall protection, select the Disable IPv4 Firewall Protection check box. By default, IPv4 firewall protection is enabled. NETGEAR recommends that you leave the firewall enabled to protect your network.
Disable Port Scan and DoS Protection	Port scan and DoS protection can protect your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. However, when port scan and DoS protection are enabled, some Apple computers might not be able to connect to the Internet. By default, port scan and DoS protection are disabled. To enable port scan and DoS protection, clear the Disable Port Scan and DoS Protection check box. Note: Enabling port scan and DoS protection might affect the performance of the modem router.
Respond to Ping on Internet Port	By default, this check box is cleared to prevent the modem router from responding to a ping from the Internet. To enable the modem router to respond to a ping, select the Respond to Ping on Internet Port check box. Note: When you allow the modem router to respond to a ping from the Internet, the modem router could be discovered by anyone and in that way become vulnerable to attacks. For optimum security, keep this check box cleared.

8. If you changed the settings, click the **Apply** button.

Your settings are saved.

Set Up a Default DMZ Server

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



WARNING:

DMZ servers pose a security risk. A computer that is designated as the default DMZ server loses firewall protection from exploits on the Internet. Once compromised, the DMZ server computer attacks other computers on your network.

The modem router discards incoming traffic from the Internet that is not a response to one of your local computers or a service that you specially set up for this purpose (see *Manage Port Forwarding to a Local Server for Services, Applications, and Games* on page 166). Instead of discarding this traffic, you can let the modem router forward the traffic to one computer on your network. This computer is called the default DMZ server.

➤ **To set up a default DMZ server:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > WAN Setup**.
The WAN Setup page displays.
6. Select the **Default DMZ Server** check box.
7. Type the IP address for the DMZ server.
8. Click the **Apply** button.
Your settings are saved and the modem router might restart.

Manage the SIP Application-Level Gateway

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

➤ **To disable the default SIP ALG:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.

5. Select **ADVANCED > Setup > WAN Setup**.

The WAN Setup page displays.

6. Select the **Disable SIP ALG** check box.

The SIP ALG is enabled by default.

7. Click the **Apply** button.

Your settings are saved.

Manage the Modem Router's LAN IP Address Settings

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

- **LAN IP address.** 192.168.0.1 (This is the same as www.routerlogin.net and www.routerlogin.com.)
- **Subnet mask.** 255.255.255.0

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. The IP address and subnet mask identify which addresses are local to a specific device and which must be reached through a gateway or modem router. You might want to change these settings if you need a specific IP subnet that one or more devices on the network use, or if competing subnets use the same IP scheme.

➤ To change the LAN IP address settings:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **<http://www.routerlogin.net>**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > LAN Setup**.

The screenshot shows the 'LAN Setup' configuration page. The 'Device Name' is set to 'C6250-100NAS'. Under 'LAN TCP/IP Setup', the IP Address is 192.168.0.1 and the IP Subnet Mask is 255.255.255.0. The 'Use Gateway as DHCP Server' checkbox is checked. The Starting IP Address is 192.168.0.10 and the Ending IP Address is 192.168.0.254. There is an empty table for 'Address Reservation' with columns for '#', 'IP Address', 'Device Name', and 'MAC Address'. Buttons for '+Add', 'Edit', and 'Delete' are located below the table.

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

Your settings are saved.

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

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

Manage IP Address Reservation

When you specify a reserved IP address for a device on the LAN, that computer always receives the same IP address each time it accesses the modem router's DHCP server. NETGEAR recommends that you assign a reserved IP address to a computer or server that requires permanent IP settings.

Reserve an IP Address

You must know the IP address and MAC address of a device for which you want to reserve an IP address.

- **To reserve an IP address:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type <http://www.routerlogin.net>.

A login window opens.

3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > LAN Setup**.
The LAN Setup page displays.
6. In the Address Reservation section, click the **Add** button.

#	IP Address	Device Name	MAC Address
1	192.168.0.11	BusinessLaptop	60:66:66:da:66:7c
2	192.168.0.12	Pavilion	d0:df:9a:9d:9b:41

7. In the **IP Address** field, type the IP address to assign to the device.
Choose an IP address from the modem router's LAN subnet, such as 192.168.0.x.

Tip: If the computer is already on your network, you can select the corresponding radio button from the Address Reservation Table. The computer's information is automatically copied into the **IP Address**, **MAC Address**, and **Device Name** fields.

8. Type the MAC address of the device.
9. Type a name for the device.
10. Click the **Add** button.

The reserved address is entered into the Address Reservation Table on the LAN Setup page.

11. On the LAN Setup page, click the **Apply** button.

Your settings are saved.

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

Change a Reserved IP Address

You can change the settings for a reserved IP address.

➤ **To change a reserved IP address:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > LAN Setup**.
The LAN Setup page displays.
6. In the Address Reservation Table, select the radio button next to the reserved address that you want to change.
7. Click the **Edit** button.
The Address Reservation page displays.
8. Change the settings.
9. Click the **Apply** button.
The changes are entered into the Address Reservation Table on the LAN Setup page.
10. On the LAN Setup page, click the **Apply** button.
Your settings are saved.

Remove an IP Address Reservation

You can remove an IP address reservation that you no longer need.

➤ **To remove an IP address reservation:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

The BASIC Home page displays.

5. Select **ADVANCED > Setup > LAN Setup**.

The LAN Setup page displays.

6. In the Address Reservation Table, select the radio button next to the reserved address that you want to remove.
7. Click the **Delete** button.

The reserved address is removed from the Address Reservation Table.

8. Click the **Apply** button.

Your settings are saved.

Manage the IPv6 LAN Settings

You can manage the IPv6 LAN settings only if the cable Internet provider assigns an IPv6 Internet address to the modem router. If the cable Internet provider assigns only an IPv4 Internet address to the modem router, you can skip this section.

If the cable Internet provider assign an IPv6 IP address to the modem router, you can specify how the modem router must assign IPv6 addresses to the devices on your home network (the LAN) and you can enable or disable the IPv6 firewall.

➤ To manage the IPv6 LAN settings:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.

A login window opens.

3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

The BASIC Home page displays.

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



In the previous figure shows, the **System Delegated Prefix** field shows an IPv6 address and prefix that were delegated by the cable Internet provider.

Note: If the modem router does not obtain an IPv6 address, all options onscreen are masked out.

6. Select an IP Address Assignment radio button:
 - **Use DHCP Server.** The modem router assigns IPv6 addresses to the devices on your home network (the LAN) through a DHCP server. This method passes more information to LAN devices, but some IPv6 systems might not support the DHCPv6 client function.
 - **Auto Config.** The modem router configures the IPv6 addresses to the devices on your home network automatically. This is the default setting.
7. To disable the IPv6 firewall protection, select the **Disable IPv6 Firewall Protection** check box.

IPv6 firewall protection can secure your network against malicious packets and is enabled by default. NETGEAR recommends that you leave the firewall enabled to protect your network.

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

Change the Modem Router's Device Name

The modem router's default device name is C6250-100NAS. This device name displays in a file manager when you browse your network.

➤ **To change the modem router's device name:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > LAN Setup**.
The LAN Setup page displays.
6. In the **Device Name** field, enter a new name.
7. Click the **Apply** button.
Your settings are saved.

Manage the Built-In DHCP Server

By default, the modem router functions as a DHCP server. The modem router assigns IP, DNS server, and default gateway addresses to all devices connected to the LAN. The assigned default gateway address is the LAN address of the modem router.

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

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

➤ **To disable the built-in DHCP server:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.

3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > LAN Setup**.
The LAN Setup page displays.
6. Clear the **Use Gateway as DHCP Server** check box.
7. Click the **Apply** button.
Your settings are saved.

Manage the DHCP Server Address Pool

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

These addresses must be part of the same IP address subnet as the modem router's LAN IP address. The default DHCP address pool is 192.168.0.10–192.168.0.254, with IP address 192.168.0.10 reserved for ReadySHARE. The first IP address that the DHCP server can assign to an attached device is 192.168.0.11.

The modem router delivers the following parameters to any LAN device that requests DHCP:

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

➤ To specify the pool of IP addresses that the modem router assigns:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Setup > LAN Setup**.

The screenshot shows the 'LAN Setup' configuration page. The 'Device Name' is 'C6250-100NAS'. Under 'LAN TCP/IP Setup', the 'Use Gateway as DHCP Server' checkbox is checked. The 'Starting IP Address' is 192.168.0.10 and the 'Ending IP Address' is 192.168.0.254. The 'IP Address' is 192.168.0.1 and the 'IP Subnet Mask' is 255.255.255.0. An 'Address Reservation' table is visible at the bottom with columns for #, IP Address, Device Name, and MAC Address. Buttons for '+ Add', 'Edit', and 'Delete' are at the bottom right.

6. Make sure that the **Use Gateway as DHCP Server** check box is selected.
This check box is selected by default.
7. Specify the range of IP addresses that the modem router assigns:
 - In the **Starting IP Address** field, enter the lowest number in the range.
This IP address must be in the same subnet as the modem router. By default, the starting IP address is 192.168.0.2.
 - In the **Ending IP Address** field, enter the number at the end of the range of IP addresses.
This IP address must be in the same subnet as the modem router. By default, the ending IP address is 192.168.0.254.
8. Click the **Apply** button.
Your settings are saved.

Manage Universal Plug and Play

Universal Plug and Play (UPnP) enables devices, such as Internet devices and computers, to 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, NETGEAR recommends that you keep UPnP enabled, which is the default setting.

➤ **To manage Universal Plug and Play:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > UPnP**.

Active	Protocol	Int. Port	Ext. Port	IP Address
Yes	UDP	64014	64014	192.168.100.123
Yes	UDP	62648	62648	192.168.100.143
Yes	UDP	50995	50995	192.168.100.143
Yes	UDP	51501	51501	192.168.100.123
Yes	UDP	30249	30249	192.168.100.143
Yes	TCP	30249	30249	192.168.100.143

The previous figure shows sample entries in the UPnP Portmap Table.

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

6. To turn off UPnP, clear the **Turn UPnP On** check box.
By default, this check box is selected. If you clear the **Turn UPnP On** check box, the modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the modem router.
7. To change the advertisement period, in the **Advertisement Period** field, enter a new period in minutes.

The advertisement period specifies how often the modem 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 can obtain current device status

at the expense of additional network traffic. Longer durations can compromise the freshness of the device status but can significantly reduce network traffic.

8. To change the advertisement time to live value, in the **Advertisement Time to Live** field, enter a new value 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 is 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.

9. Click the **Apply** button.

Your settings are saved.

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

The information onscreen is updated.

Manage the Modem Router and Monitor Your Network

7

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

This chapter includes the following sections:

- *View the Status and Statistics of the Modem Router*
- *View Devices Currently on the Network*
- *View WiFi Channels in Your Environment*
- *View WiFi Networks in Your Environment*
- *View and Manage the Log*
- *Change the Password*
- *Manage the Device Settings File of the Modem Router*
- *Return the Modem Router to Its Factory Default Settings*
- *Reboot the Modem Router*
- *Monitor and Meter Internet Traffic*
- *Manage the Modem Router Remotely*

For additional management information, see the following sections:

- For information about diagnostic tools, see *Perform Diagnostics* on page 181.
- For information about the event log, see *View and Manage the Event Log* on page 187.
- For information about turning off router mode to enable the modem router to function as a bridge to another router, see *Cable the Modem Router to a Router and Use Bridge Mode* on page 17.

View the Status and Statistics of the Modem Router

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

View the Cable Information and Internet Port and WiFi Status

The ADVANCED Home page displays cable information, the Internet port status, and WiFi settings for the radio of the main and guest networks.




- **To view information about the modem router, Internet port, and WiFi settings:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > ADVANCED Home**.

AC1600 WiFi Cable Modem Router

The screenshot shows the 'ADVANCED' settings page of the Netgear AC1600 WiFi Cable Modem Router. On the left, there is a navigation menu with options: 'ADVANCED Home', 'WPS Wizard', 'Setup', 'USB Storage', 'Security', 'Administration', and 'Advanced Setup'. The main content area is divided into six panels, each with a status icon in the top left corner:

- Cable Information** (Green checkmark): Hardware Version 1.02, Firmware Version V1.01.05, Cable Modem Serial Number BTA0517R000A5, CM Certificate Installed, CM MAC c0:ff:d4:ea:4c:b8, LAN Port, MAC Address c0:ff:d4:ea:4c:ba, IP Address/Mask 192.168.0.1/24, DHCP On. Buttons: Factory reset, Reboot.
- Internet Port** (Green checkmark): MAC Address c0:ff:d4:ea:4c:b9, IP Address/Mask 192.168.15.3/25, Connection DHCP Client, Default Gateway 192.168.15.1, Domain Name Server 172.29.16.12, 4.2.2.2. Buttons: Show Statistics, Connection Status.
- Wireless Settings (2.4GHz)** (Green checkmark): Name (SSID) NETGEAR34, Region United States, Channel 7, Mode Up to 54 Mbps, Wireless AP On, Broadcast Name On, Wi-Fi Protected Setup Configured.
- Wireless Settings (5GHz)** (Green checkmark): Name (SSID) NETGEAR34-5G, Region United States, Channel 149 + 153 (P) + 157 + 161, Mode Up to 1.3 Gbps, Wireless AP On, Broadcast Name On, Wi-Fi Protected Setup Configured.
- Guest Network (2.4 GHz)** (Amber exclamation mark): Name (SSID) NETGEAR-Guest, Wireless AP On, Broadcast Name On, Allow guest to access My Local Network Off.
- Guest Network (5 GHz)** (Red X): Name (SSID) ---, Wireless AP Off, Broadcast Name ---, Allow guest to access My Local Network ---.

The color of the icon indicates the following status:

- A green flag  indicates that the cable connection or Internet connection is fine and no problems exist. For a WiFi network, the network is enabled and secured.
- A red X  indicates that configuration problems exist for the cable connection or Internet connection or the connection is down. For a WiFi network, the network is disabled or down.
- An amber exclamation mark  indicates that the cable port or 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.

The following table describes the panes on the ADVANCED Home page.

Field	Description
Cable Information	
Hardware Version	The modem router hardware version.
Firmware Version	The version of the router firmware. If you upgrade the router firmware on the modem router, the version changes.
Cable Modem Serial Number	The modem router serial number.
CM Certificate	The modem router digital certificate.
CM MAC	The cable port Media Access Control (MAC) address. This address is the unique physical address of the management interface that the cable provider uses to manage the modem router. This MAC address is on the product label.
LAN Port The settings of the Ethernet LAN port. For information about how to configure the LAN settings, see Manage the Modem Router's LAN IP Address Settings on page 84 and Manage the Built-In DHCP Server on page 90.	
MAC Address	The Ethernet LAN port MAC address. This address is the unique physical address that is assigned to the Ethernet LAN port.
IP Address	The IP address that the Ethernet LAN port uses. The default IP address is 192.168.0.1.
DHCP	Displays whether the DHCP server of the modem router is enabled for devices that are attached to the LAN.
Internet Port The settings of Internet port. For information about how to configure the Internet settings, see View or Manually Set Up the IPv4 Internet Settings on page 30.	
MAC Address	The Internet port MAC address. This address is the unique physical address that is assigned to the Internet port.
IP Address/Mask	The IP address and subnet mask (in the /xx format) that the cable Internet port uses. If this field does not display an address or displays 0.0.0.0 as the address, the modem router cannot provide an Internet connection over the cable Internet port.
Connection	The type of network address, which is either a fixed IP address or an IP address that the modem router obtains dynamically from the DHCP server of the cable service provider. In the latter case, the field displays DHCP Client.
Default Gateway	The IP address of the cable service provider's gateway that the cable Internet port uses.
Domain Name Server	The IP addresses of the Domain Name System (DNS) servers that the cable Internet port uses.

AC1600 WiFi Cable Modem Router

Field	Description
<p>Wireless Settings (2.4GHz)</p> <p>The settings of the WiFi port for the 2.4 GHz band of the main network. For information about how to configure the settings of the main network, see Manage the Basic WiFi Settings and WiFi Security of the Main Network on page 36, Control the WiFi Radios on page 155, and Manage the Advanced WiFi Settings on page 159.</p>	
Name (SSID)	The WiFi network name for the 2.4 GHz band of the main network.
Region	The location (country).
Channel	The channel that the 2.4 GHz band of the main network uses.
Mode	The WiFi mode in which the 2.4 GHz band operates for both the main network and the guest network.
Wireless AP	Displays whether the 2.4 GHz band of the main network is enabled. If the 2.4 GHz band is disabled, the 2.4 GHz WiFi LED is off. For information about enabling the 2.4 GHz band, see Enable or Disable the WiFi Radios on page 155.
Broadcast Name	Displays whether the 2.4 GHz band of the main network broadcasts its SSID.
Wi-Fi Protected Setup	Displays whether the modem router keeps its existing WiFi settings when you use WPS to connect a device to the 2.4 GHz band of the main network: <ul style="list-style-type: none"> • Configured. The modem router keeps its existing WiFi settings. This is the default setting. • Not configured. The modem router generates a random SSID and passphrase and changes the security mode to WPA/WPA2-PSK mixed mode. For more information, see Manage WPS Settings on page 161.
<p>Wireless Settings (5GHz)</p> <p>The settings of the WiFi port for the 5 GHz band of the main network. For information about how to configure the settings of the main network, see Manage the Basic WiFi Settings and WiFi Security of the Main Network on page 36, Control the WiFi Radios on page 155, and Manage the Advanced WiFi Settings on page 159.</p>	
Name (SSID)	The WiFi network name for the 5 GHz band of the main network.
Region	The location (country).
Channel	The channel that the 5 GHz band of the main network uses.
Mode	The WiFi mode in which the 5 GHz band operates for both the main network and the guest network.
Wireless AP	Displays whether the 5 GHz band of the main network is enabled. If the 5 GHz band is disabled, the 5 GHz WiFi LED is off. For information about enabling the 5 GHz band, see Enable or Disable the WiFi Radios on page 155.
Broadcast Name	Displays whether the 5 GHz band of the main network broadcasts its SSID.

AC1600 WiFi Cable Modem Router

Field	Description
Wi-Fi Protected Setup	<p>Displays whether the modem router keeps its existing WiFi settings when you use WPS to connect a device to the 5 GHz band of the main network:</p> <ul style="list-style-type: none"> • Configured. The modem router keeps its existing WiFi settings. This is the default setting. • Not configured. The modem router generates a random SSID and passphrase and changes the security mode to WPA/WPA2-PSK mixed mode. <p>For more information, see Manage WPS Settings on page 161.</p>
<p>Guest Network (2.4 GHz)</p> <p>The settings of the WiFi port for the 2.4 GHz band of the guest network. For information about how to configure the settings of the guest network, see Manage the Basic WiFi Settings and WiFi Security of the Guest Network on page 48.</p>	
Name (SSID)	The WiFi network name for the 2.4 GHz band of the guest network.
Wireless AP	<p>Displays whether the 2.4 GHz band of the guest network is enabled.</p> <p>The WiFi LED on the front of the modem router is not affected by the status of the guest network.</p>
Broadcast Name	Displays whether the 2.4 GHz band of the guest network broadcasts its SSID.
Allow guests to see each other and access my local network	Displays whether users of the 2.4 GHz band of the guest network are allowed to access the main network.
<p>Guest Network (5 GHz)</p> <p>The settings of the WiFi port for the 5 GHz band of the guest network. For information about how to configure the settings of the guest network, see Manage the Basic WiFi Settings and WiFi Security of the Guest Network on page 48.</p>	
Name (SSID)	The WiFi network name for the 5 GHz band of the guest network.
Wireless AP	<p>Displays whether the 5 GHz band of the guest network is enabled.</p> <p>The WiFi LED on the front of the modem router is not affected by the status of the guest network.</p>
Broadcast Name	Displays whether the 5 GHz band of the guest network broadcasts its SSID.
Allow guests to see each other and access my local network	Displays whether users of the 5 GHz band of the guest network are allowed to access the main network.

View the Traffic Statistics

You can view the traffic statistics for the ports of the modem router, change the polling frequency, and stop traffic polling.

- **To view the traffic statistics for the ports of the modem router:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type <http://www.routerlogin.net>.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > ADVANCED Home**.
The ADVANCED Home page displays.
 6. In the Internet Port pane, click the **Show Statistics** button.

Show Statistics							
System Up Time		00:33:18					
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Link Up	6153254	544480	--	--	--	00:33:18
LAN1	Link Down	0	0	0	0	0	--
LAN2	Link Down						--
WLAN/2.4G	54M	7831	9737	0	2726	631	00:33:18
WLAN/5G	1.3G	6766	1	0	468	0	00:33:18
Poll Interval: 5 (secs)		Set Interval		Stop			

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

The following table describes the fields and columns of the Show Statistics pop-up window.

Field or Column	Description
System Up Time	The time elapsed since the modem router was last restarted.
Port	The statistics for the WAN port (that is, the cable Internet port that connects to the Internet), LAN (Ethernet) ports, and WLAN (WiFi) ports. For each port, the pop-up window displays the information that is described in this table.

Field or Column	Description
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.
Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	The interval at which the statistics are updated in this pop-up window.

➤ **To change the traffic statistics polling frequency or stop polling:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > ADVANCED Home**.
The ADVANCED Home page displays.
6. In the Internet Port pane, click the **Show Statistics** button.
The Show Statistics pop-up window displays.
If this window does not display, your web browser might be blocking pop-ups. If it is, change the browser settings to allow pop-ups.
7. Change the polling frequency or stop polling:
 - To change the polling frequency, do the following:
 - a. In the **Poll Interval** field, enter a time in seconds.
 - b. Click the **Set Interval** button.
 - To stop polling, click the **Stop** button.

View the Internet Port Connection Status and Release and Renew the Connection

You can view information about the cable Internet connection of the modem router. You can also release and renew the connection.

➤ **To view the status of the cable Internet connection of the modem router and release and renew the connection:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > ADVANCED Home**.
The ADVANCED Home page displays.
6. In the Internet Port pane, click the **Connection Status** button.

Connection Status	
IP Address	192.168.15.3
Subnet Mask	255.255.255.128
Default Gateway	192.168.15.1
DHCP Server	172.29.16.12
DNS Server	172.29.16.12, 4.2.2.2, ---,---,---,---
Lease Obtained	D: 00 H: 12 M: 00 S: 00
Lease Expires	---:---:---:---

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

The following table describes the fields of the Connection Status pop-up window.

Field	Description
IP Address	The IP address that is assigned by the cable service provider to the modem router.
Subnet Mask	The subnet mask that is assigned by the cable service provider to the modem router.

Field	Description
Default Gateway	The IP address of the default gateway of the cable service provider that the modem router communicates with.
DHCP Server	The IP address of the Dynamic Host Configuration Protocol (DHCP) server of the cable service provider that assigns IP addresses.
DNS Server	The IP address of the Domain Name System (DNS) server of the cable service provider that provides translation of network names to IP addresses.
Lease Obtained	The day and time that the lease was obtained.
Lease Expires	The day and time that the lease expires.

- To release the connection, click the **Release** button.

The connection with your cable service provider is shut down, as is your Internet connection.

- To renew the connection, click the **Renew** button.

The connection with your cable service provider is reestablished, as is your Internet connection. If a DHCP connection with your cable service provider exists, the modem router receives a new DHCP lease and might receive a new IP address.

- Click the **Close Window** button.

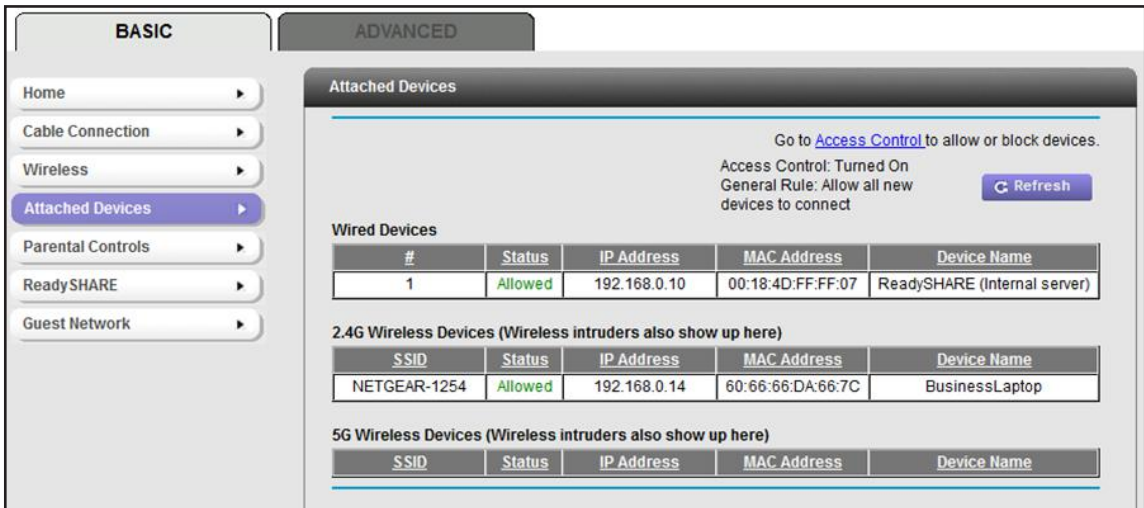
The pop-up window closes.

View Devices Currently on the Network

You can view the active wired devices, 2.4 GHz WiFi devices, and 5 GHz WiFi devices in the network. If you do not recognize a device, it might be an intruder. If it is an intruder, make sure that your WiFi security is set up correctly (see [Manage the Basic WiFi Settings and WiFi Security of the Main Network](#) on page 36) or set up access control to secure your network (see [Allow or Block Access to Your Network](#) on page 58).

➤ To display the connected wired and WiFi devices:

- Launch an Internet browser from a computer or WiFi device that is connected to the network.
- Type **http://www.routerlogin.net**.
A login window opens.
- Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
- Click the **OK** button.
The BASIC Home page displays.
- Select **Attached Devices**.



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

The following table describes the fields of the three tables on the Attached Devices page.

Field	Description
SSID	The WiFi network name (for WiFi devices only).
Status	The access control status (Allowed or Blocked, that is, blocked from reconnecting after the device disconnects).
IP Address	The IP address that the modem router assigned to the device when it joined the network. This address can change when a device is disconnected and rejoins the network.
MAC Address	The unique MAC address of the device. The MAC address does not change and is usually shown on the product label.
Device Name	The device name, if detected.

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

The information onscreen is updated.

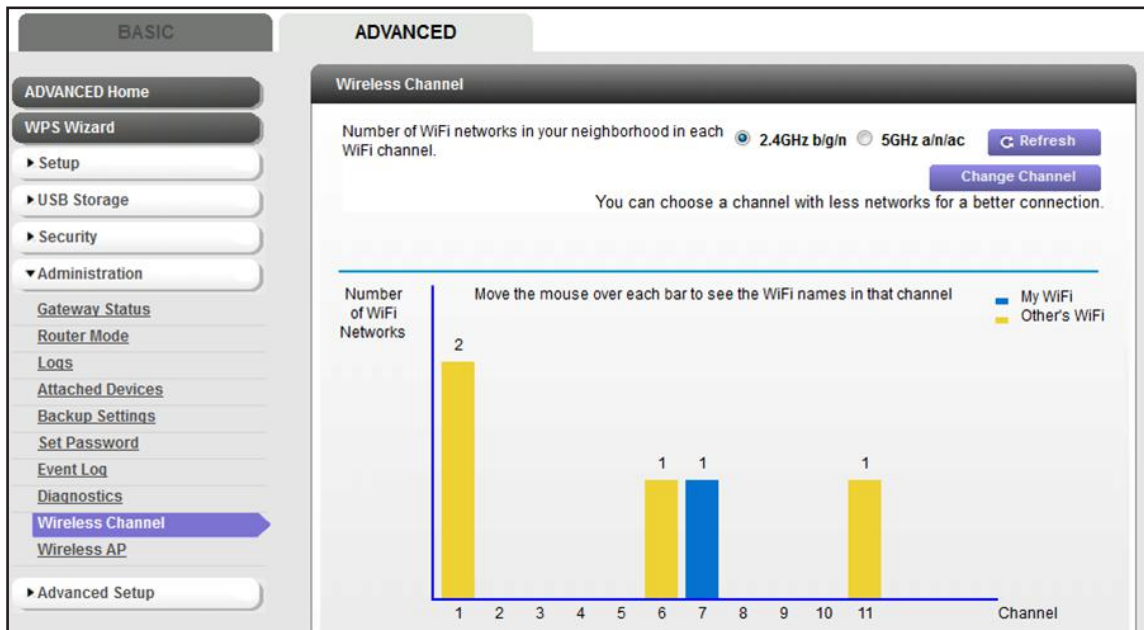
View WiFi Channels in Your Environment

You can view the active WiFi channels in your environment, including the channels that the modem router is broadcasting on. If several WiFi networks in your environment are using the same channel as the one that the modem router is using, interference might occur. In that situation, you might want to change the channel that the modem router is using.

Note: Many countries and geographic locations implement laws or guidelines about which channels can be used. Depending on your location, some channels might not be available.

➤ **To view the WiFi channels in your environment:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Administration > Wireless Channel**.



By default, the **2.4GHz b/g/n** radio button is selected and the page displays the active channels in the 2.4 GHz band. The number above a bar indicates the number of WiFi networks that broadcast in the channel.

The channel that the WiFi network of the modem router is using displays in blue. The channels that other WiFi network in your environment are using display in yellow.

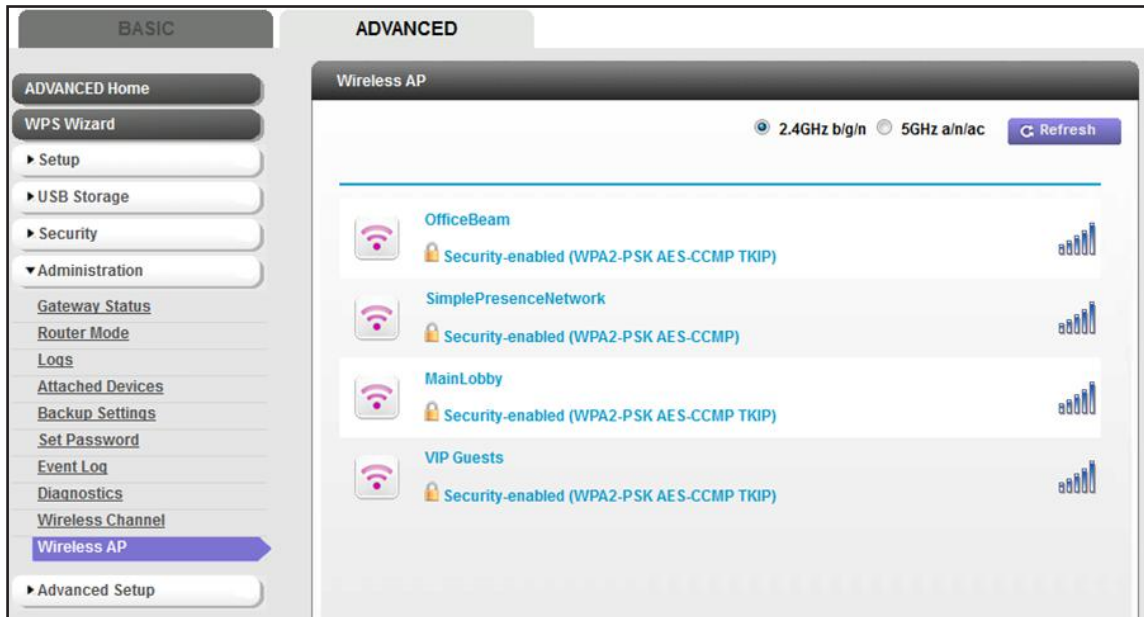
6. To view the WiFi name (SSID) that operates in a channel, point to a bar.

7. To display the active channels and channel information in the 5 GHz band, select the **5GHz a/n/ac** radio button.
8. To refresh the page, click the **Refresh** button.
The information onscreen is updated.
9. To change the channel that a radio of the modem router is using, click the **Change Channel** button.
The Wireless Setup page displays.
For information about changing the WiFi settings for the main WiFi network, including the channel, see *Manage the Basic WiFi Settings and WiFi Security of the Main Network* on page 36.

View WiFi Networks in Your Environment

You can view the WiFi networks that are being broadcast by access points (APs) in your environment. These are access points other than the modem router. For each WiFi network, the security level and the signal strength are displayed.

- **To view the WiFi networks in your environment:**
1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > Administration > Wireless AP**.



By default, the **2.4GHz b/g/n** radio button is selected and the page displays the WiFi networks in the 2.4 GHz band.

6. To display the WiFi networks in the 5 GHz band, select the **5GHz a/n/ac** radio button.
7. To refresh the page, click the **Refresh** button.

The information onscreen is updated.

View and Manage the Log

The log is a detailed record of websites that users accessed, attempts to access blocked sites, modem router operation, DoS attacks and port scans, WiFi access, and other information. Up to 256 entries can be stored in the log.

If you enabled email notification, you receive these logs in an email message. For more information, see [Set Up Security Event Email Notification](#) on page 78.

Note: For information about the event log, which is a log that records events that occur between the modem router and the cable service provider's cable modem termination system (CMTS), see [View and Manage the Event Log](#) on page 187.

- **To view, send, or clear the log and specify what is included in the log:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type <http://www.routerlogin.net>.

A login window opens.

3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Administration > Logs**.

Description	Count	Last Occurrence	Target	Source
[Time Of Day established]	6	Fri Dec 05 12:09:44 2014	---	---
[Public Network Interface up]	1	Fri Dec 05 12:10:15 2014	---	---
[Firewall Up]	1	Fri Dec 05 12:10:15 2014	---	---
[Time Of Day established]	2	Fri Dec 05 12:32:02 2014	---	---
[Public Network Interface up]	1	Fri Dec 05 12:32:36 2014	---	---
[Firewall Up]	1	Fri Dec 05 12:32:36 2014	---	---
[FAILURE: User interface login]	1	Fri Dec 05 13:09:01 2014	192.168.0.1:80	192.168.0.22:58669
[SUCCESS: User interface login]	1	Fri Dec 05 13:09:08 2014	192.168.0.1:80	192.168.0.22:58670
[Time Of Day established]	1	Fri Dec 05 13:18:40 2014	---	---
[Public Network Interface up]	1	Fri Dec 05 13:19:13 2014	---	---
[Firewall Up]	1	Fri Dec 05 13:19:13 2014	---	---
[Time Of Day established]	1	Fri Dec 05 13:23:07 2014	---	---

The Logs page displays a table that shows for each event a description, the number of times the events occurred, the date and time of the last occurrence, the target IP address and port, and the source IP address and port.

6. Scroll down.

The bottom of the page shows check boxes and buttons.

Refresh Clear Log Send Log

Include in Log

- Attempted access to blocked sites and services
- Connections to the Web-based interface of this Gateway
- Gateway operation (startup, get time etc)
- Known DoS attacks and Port Scans
- Port Forwarding / Port Triggering
- Turn off wireless signal by schedule

7. To specify which types of events are logged, select or clear the check boxes.

By default, all the check boxes are selected and the associated events are logged.

8. If you make any changes, click the **Apply** button at the top of the page.

Your settings are saved.

9. To refresh the page, click the **Refresh** button.

The information onscreen is updated.

10. To email the log immediately, click the **Send Log** button.

This feature can be useful for testing your email settings. For this feature to function, you first must enable email notification. For more information, see [Set Up Security Event Email Notification](#) on page 78.

11. To clear the log entries, click the **Clear Log** button.

All entries are removed from the table.

Change the Password

The user name to access the modem router is admin, and its default password is password. NETGEAR recommends that you set a more secure password.

A secure password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. The password must contain at least 4 characters and can contain a maximum of 15 characters.

Note: This change of password is not the same as changing the password (key) for WiFi access. The product label shows your unique WiFi network name (SSID) and password for WiFi access.

➤ To change the password for the modem router:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and **password** for the password.
If you already changed the password and want to change it again, type your personalized password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Administration > Set Password**.

6. Type the old password.
7. Type the new password twice.
8. Click the **Apply** button.

Your settings are saved.

Manage the Device Settings File of the Modem Router

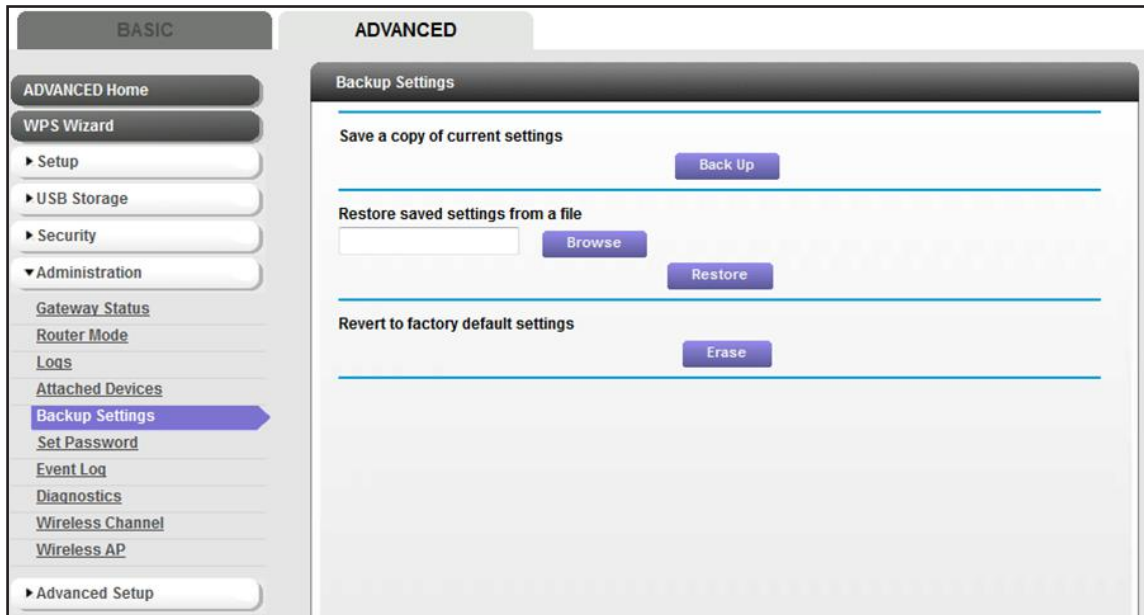
The settings of the modem router are stored within the modem router in a device settings file. You can back up (save) this file to your computer or restore it from a previously backed-up file.

Back Up the Settings

You can save a copy of the current settings.

➤ To back up the modem router's settings:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Administration > Backup Settings**.

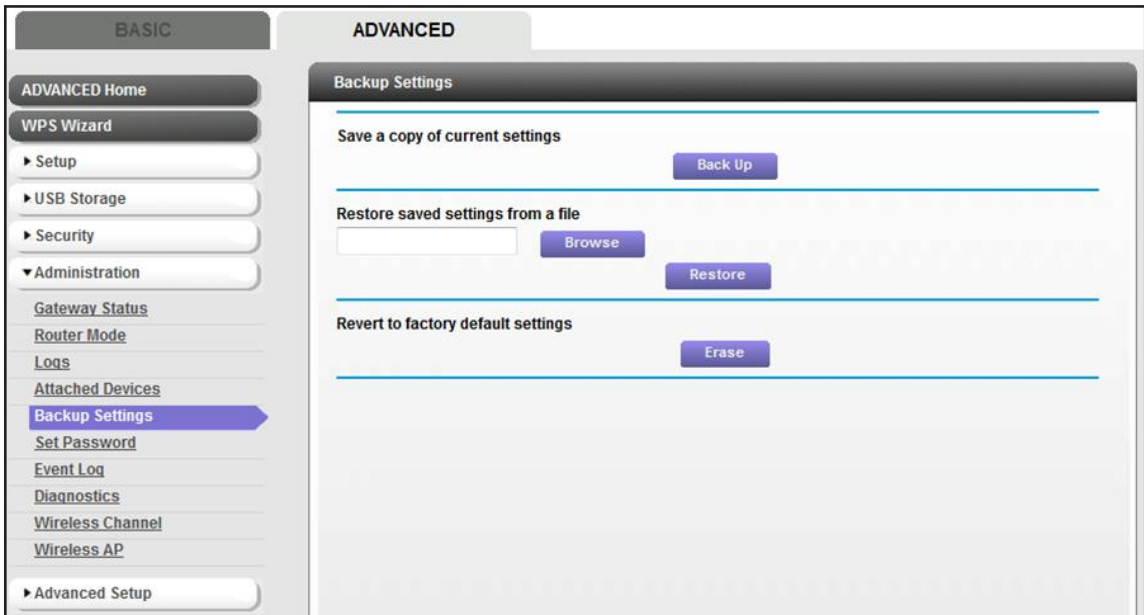


6. Click the **Back Up** button.
7. Choose a location to store the file on a device on your network.
The default name of the backup file is `NETGEAR_C6250-100NAS.cfg`.
8. To save the file, follow the directions of your browser.

Restore the Settings

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

- **To restore settings that you backed up:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > Administration > Backup Settings**.



6. Enter the full path to the file on your network or click the **Browse** button to find the file.

The default name of the backup file from which you can restore the settings is `NETGEAR_C6250-100NAS.cfg`.

7. Follow the directions of your browser to locate the file, and select it.
8. Click the **Restore** button.

The settings are uploaded to the modem router. When the restoration is complete, the modem router reboots.



WARNING:

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

Return the Modem Router to Its Factory Default Settings

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

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

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

However, if you cannot find the LAN IP address or lost the password to access the modem router, you must use the **Reset** button.

After you reset the modem router to factory default settings, the user name is admin, the password is password, the LAN IP address is 192.168.0.1 (which is the same as www.routerlogin.net and www.routerlogin.com), and the DHCP server is enabled. For a list of factory default settings, see *Factory Default Settings* on page 195.

Use the Reset Button



CAUTION:

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

➤ To reset the modem router to factory default settings:

1. On the back panel of the modem router, look for the small hole in which the **Reset** button is located.

For more information about the location of the **Reset** button, see *Back Panel* on page 12.

2. Insert a straightened paper clip into the hole and press for at least eight seconds.
3. Release the button.

The modem router resets and restarts. This process takes about one minute.



WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the restoration. For example, do not turn off the modem router.

Erase the Settings



CAUTION:

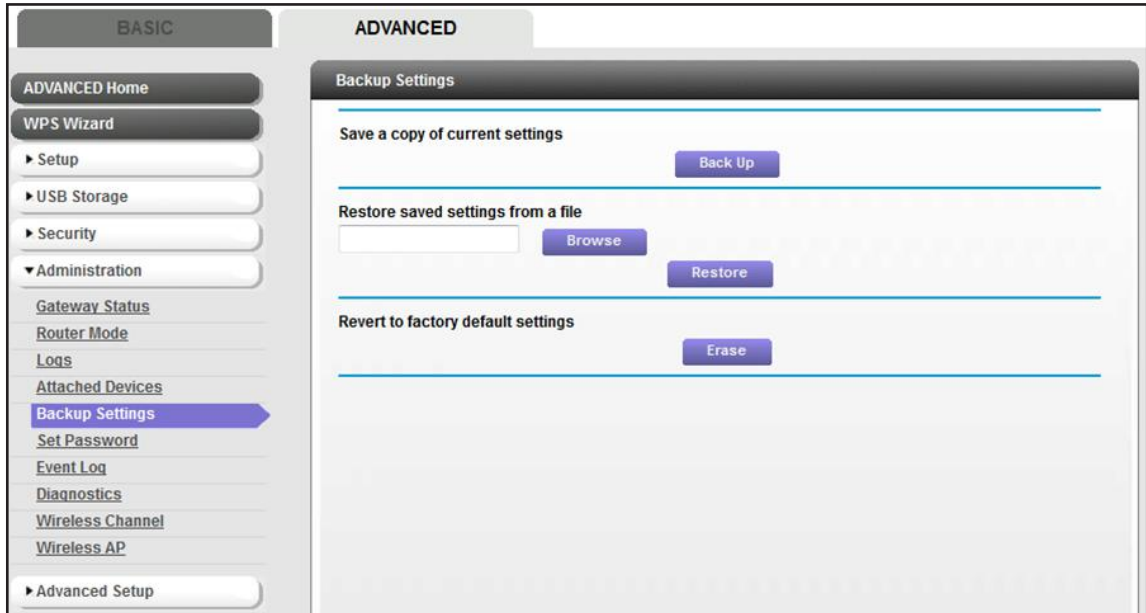
This process erases all settings that you configured in the modem router.

➤ To erase the settings:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

- Click the **OK** button.
The BASIC Home page displays.
- Select **ADVANCED > Administration > Backup Settings**.



- Click the **Erase** button.
A warning message displays.
- To confirm the action, click the **Yes** button.
The configuration is reset to factory default settings and the Updating Settings page displays. When the restoration is complete, the modem router reboots.



WARNING:

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

Reboot the Modem Router

You can reboot the modem router from the web management interface.

- **To reboot the modem router from the web management interface:**
 - Launch an Internet browser from a computer or WiFi device that is connected to the network.
 - Type **http://www.routerlogin.net**.
A login window opens.

3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > ADVANCED Home**.
The ADVANCED Home page displays.
6. In the Cable Information pane, click the **Reboot** button.
A warning message displays.
7. To confirm the reboot, click the **OK** button.
The modem router reboots.

**WARNING:**

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

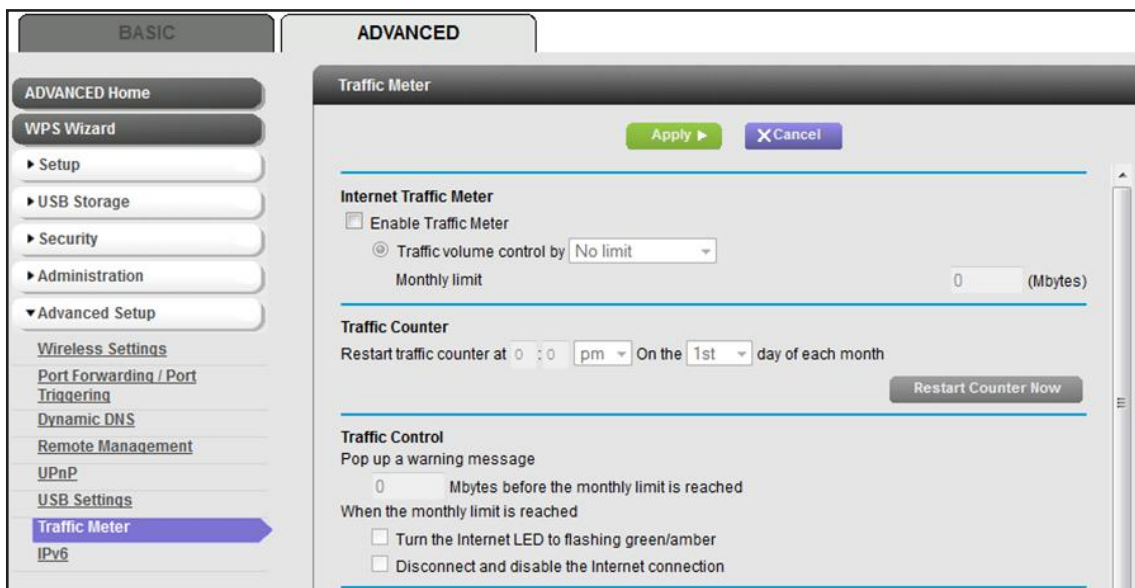
Monitor and Meter Internet Traffic

Traffic metering allows you to monitor the volume of Internet traffic that passes through the modem router Internet port. With the traffic meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

Start the Traffic Meter Without Traffic Volume Restrictions

You can monitor the traffic volume without setting a limit.

- **To start or restart the traffic meter without configuring traffic volume restrictions:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > Advanced Setup > Traffic Meter**.



6. Select the **Enable Traffic Meter** check box.

By default, no traffic limit is specified and the traffic volume is not controlled.

7. In the Traffic Counter section, set the traffic counter to begin at a specific time and date in each month.
8. To start the traffic counter immediately, click the **Restart Counter Now** button.
9. Click the **Apply** button.

Your settings are saved and the WiFi connection restarts. Any WiFi devices that were connected to the network must reconnect.

The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see [View the Traffic Statistics and Traffic Status](#) on page 117.

View the Traffic Statistics and Traffic Status

If you enabled the traffic meter (see [Start the Traffic Meter Without Traffic Volume Restrictions](#) on page 116), you can view the traffic statistics and traffic status.

➤ To view the traffic statistics and status of the traffic meter:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Traffic Meter**.

The Traffic Meter page displays.

6. Scroll down to the Internet Traffic Statistics section.

Internet Traffic Statistics			
Start Date/Time: -----			
Current Date/Time: -----			
Traffic Volume Left: No Limit			
Period	Traffic Volume (Mbytes)		
	Upload/Avg	Download/Avg	Total/Avg
Today	0.00	0.00	0.00
Yesterday	0.00	0.00	0.00
This week	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00
This month	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00
Last month	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00

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.

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

The information onscreen is updated.

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

The Traffic Status pop-up window displays.

Restrict Internet Traffic

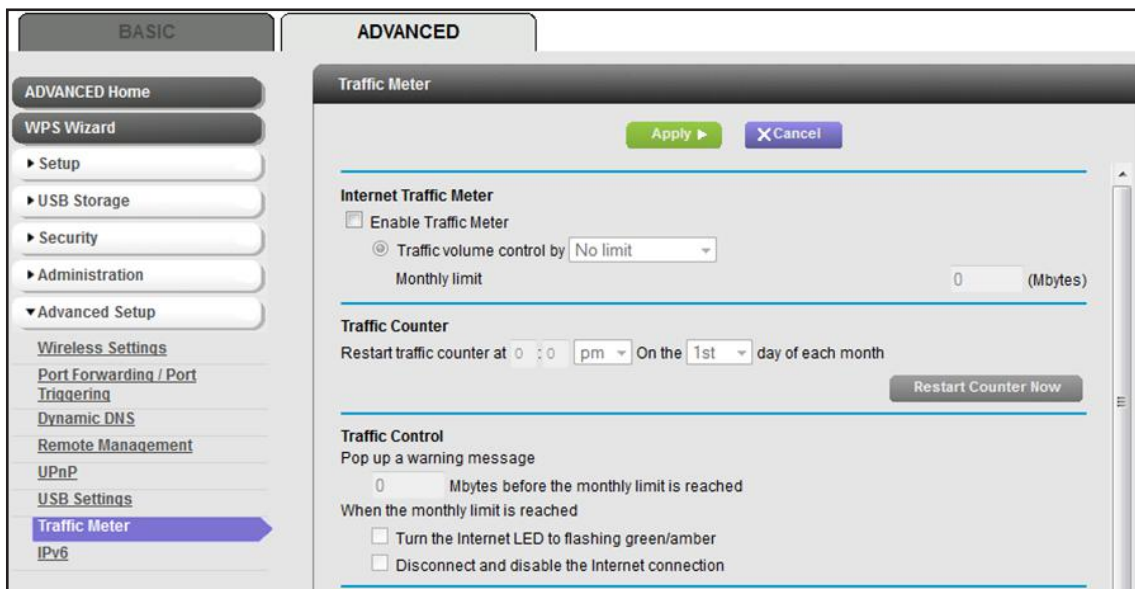
If traffic usage reaches a threshold, the modem router can disconnect and disable the Internet connection to ensure that traffic usage does not exceed the threshold.

➤ To restrict the Internet traffic:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.

The BASIC Home page displays.

5. Select **ADVANCED > Advanced Setup > Traffic Meter**.



6. Select the **Enable Traffic Meter** check box.
7. From the **Traffic volume control by** 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. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.
10. To start the counter immediately, click the **Restart Counter Now** button.
11. To enable the modem router to generate a warning message, in the Traffic Control section, enter a value in Mbytes or minutes.

The modem router generates a warning message when the balance falls under the value that you enter. This setting is optional. By default, the value is 0 and the modem router does not generate a warning message.

12. Select one or more of the following actions to occur when the limit is reached:
 - **Turn the Internet LED to flashing green/amber**. This setting is optional. When the traffic limit is reached, the Internet LED blinks alternating green and amber.
 - **Disconnect and disable the Internet connection**. This setting is optional. When the traffic limit is reached, the Internet connection is disconnected and disabled.
13. Click the **Apply** button.

Your settings are saved and the WiFi connection restarts. Any WiFi devices that were connected to the network must reconnect.

The Internet Traffic Statistics section helps you to monitor the data traffic. For more information, see [View the Traffic Statistics and Traffic Status](#) on page 117.

Unblock the Traffic Meter After the Traffic Limit Is Reached

If you configured the traffic meter to disconnect and disable the Internet connection after the traffic limit is reached, you cannot access the Internet until you unblock the traffic meter.



CAUTION:

If your ISP set a traffic limit, your ISP might charge you for the overage traffic.

➤ To unblock the traffic meter:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Traffic Meter**.
The Traffic Meter page displays.
6. In the Traffic Control section, clear the **Disconnect and disable the Internet connection** check box.
7. Click the **Apply** button.
Your settings are saved.

Manage the Modem Router Remotely

The remote management feature lets you update or check the status of your modem router through a secure HTTP (HTTPS) connection over the Internet. For enhanced security, restrict access to as few external IP addresses as practical.

Note: Be sure to change the modem router default login password to a secure password. For more information, see *Change the Password* on page 110.

➤ **To set up remote management:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Remote Management**.

The screenshot shows the 'Remote Management' configuration page. On the left is a navigation menu with 'Remote Management' highlighted. The main content area has a 'Turn Remote Management On' checkbox. Below it, the 'Remote Management Address' is 'https://10.1.112.79:8443'. Under 'Allow Remote Access By', the 'Everyone' radio button is selected. The 'Port Number' field contains '8443'. There are 'Apply' and 'Cancel' buttons at the top.

The **Remote Management Address** field shows the IP address that is assigned to the modem router and the secure port number, both of which are required to log in to the modem router from a remote location.

6. Select the **Turn Remote Management On** check box.
7. Specify the external IP address or addresses from which the modem router can be managed remotely:
 - To specify access for a single IP address on the Internet, do the following:
 - a. Select the **Only This Computer** radio button.
 - b. Enter the IP address from which access is allowed.
 - To specify access for a range of IP addresses on the Internet, do the following:
 - a. Select **IP Address Range** radio button.
 - b. In the **From** field, enter the start IP address of the range from which access is allowed.
 - c. In the **To** field, enter the end IP address of the range from which access is allowed.

- To specify access for all IP addresses on the Internet, keep the **Everyone** radio button selected.

This is the default setting.

8. In the **Port Number** field, specify the port number for accessing the web management interface.

Normal secure web browser access uses the standard HTTPS service port 443. For greater security, enter a custom port number for the remote web management interface. Choose a number from 1024 to 65535 but do not use the number of any common service port. The default port number is 8443.

9. Click the **Apply** button.

Your settings are saved. After a while, the external IP address and port number display in the **Remote Management Address** field.

When you access your modem router from the Internet, type your modem router's external (WAN) IP address in your browser's address or location field followed by a colon (:) and the custom port number. For example, if your external address is 203.0.113.123 and you use port number 8443, enter **https://203.0.113.123:8443** in your browser.

Share a Storage Device

8

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

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

The chapter includes the following sections:

- *USB Device Requirements*
- *Connect a USB Device to the Modem Router*
- *Access a Storage Device Connected to the Modem Router*
- *Manage Access to a Storage Device*
- *Enable FTP Access Within Your Network*
- *View Network Folders on a Device*
- *Add a Network Folder on a Storage Device*
- *Change a Network Folder, Including Read and Write Access, on a USB Drive*
- *Approve USB Devices*
- *Safely Remove a USB Device*
- *Enable the Media Server*

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

USB Device Requirements

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

kbserver.netgear.com/readysware.

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

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

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

The modem router supports the following file system types with read-only access:

- HFS
- HFS+

Connect a USB Device to the Modem Router

ReadySHARE lets you access and share a USB device that is connected to a USB port on the modem router. (If your USB device uses special drivers, it is not compatible.) The USB 2.0 port is on the back panel of the modem router.

➤ To connect a USB device:

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

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

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

Access a Storage Device Connected to the Modem Router

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

➤ To access the device from a Mac:

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

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

When you connect the storage device to the modem router's port, it might take up to two minutes before the storage device is ready for sharing. By default, the 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**.
4. In the **Server Address** field, enter **smb://readyshare**.
5. When prompted, select the **Guest** radio button.
6. Click the **Connect** button.

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

➤ To access the device from a Windows computer:

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

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

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

3. Launch a web browser from a computer that is connected to the network.
4. In the address field of the browser, enter **\\readyshare**.

Windows file manager automatically opens and displays the files and folders on the device.

Manage Access to a Storage Device

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

➤ **To specify the storage device access settings:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > USB Storage > Advanced Settings**.

The screenshot shows the 'ADVANCED' settings page for 'USB Storage (Advanced Settings)'. The left sidebar has 'Advanced Settings' selected. The main content area includes 'Apply' and 'Refresh' buttons, and input fields for 'Network/Device Name' (readyshare) and 'Workgroup' (Workgroup). Below these are two tables:

Enable	Access Method	Link	Port
<input checked="" type="checkbox"/>	Network Connection	\\readyshare	-
<input checked="" type="checkbox"/>	HTTP	http://readyshare.routerlogin.net/shares	80
<input type="checkbox"/>	HTTPS (via internet)	https://0.0.0.0/shares	443
<input type="checkbox"/>	FTP	ftp://readyshare.routerlogin.net/shares	21
<input type="checkbox"/>	FTP (via internet)	ftp://0.0.0.0/shares	21

	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
<input checked="" type="radio"/>	\\readyshare\USB_Storage	All - no password	All - no password	U:\	STORE N GO	3.72 G	617 M

Buttons at the bottom include 'Edit', 'Create Network Folder', 'Delete', and 'Safely Remove USB Device'.

The previous figure shows a USB device attached to the modem router.

6. In the **Network/Device Name** field, enter the name that is used to access the USB device or devices that are connected to the modem router. By default, the name is readyshare.

- In the **Workgroup** field, enter the name of the workgroup that the USB device or devices are members of. By default, the name is WORKGROUP. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows.

If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here.

- Enable or disable access methods by selecting or clearing the corresponding check boxes and specifying access to the storage device as described in the following table.

Access Method	Description
Network Connection	Enabled by default. You can type <code>\\readyshare</code> to access the storage device within your network. If you change the name in the Network/Device Name field from readyshare to another name, the link changes accordingly.
HTTP	Enabled by default. You can type <code>http://readyshare.routerlogin.net/shares</code> to access the USB device within your network and download or upload files. In this URL, readyshare is the name that is specified in the Network/Device Name field. If you change the name in the Network/Device Name field from readyshare to another name, the link changes accordingly. You can also click the link that is shown in the Link column. The fixed port is number is 80.
HTTPS (via Internet)	Disabled by default. If you enable this feature, remote users can type <code>https://<public IP address>/shares</code> to access the USB device over the Internet. <code><public IP address></code> is the external or public IP address that is assigned to the modem router (for example, 1.1.10.102). This feature supports file uploading only. The default port is number 443, which you can change.
FTP	Enabled by default. You can type <code>ftp://readyshare.routerlogin.net/shares</code> to access the USB device within your network and download or upload files. In this URL, readyshare is the name that is specified in the Network/Device Name field. If you change the name in the Network/Device Name field from readyshare to another name, the link changes accordingly. You can also click the link that is shown in the Link column. The fixed port is number is 21.
FTP (via Internet)	Disabled by default. If you enable this feature, remote users can type <code>ftp://<public IP address>/shares</code> to access the USB device over the Internet and download or upload files. <code><public IP address></code> is the external or public IP address that is assigned to the modem router (for example, 1.1.10.102). The default port is number 21, which you can change. If you set up Dynamic DNS (see Set Up and Manage Dynamic DNS on page 147), you can also type a URL domain name. For example, if your domain name is MyName and you use the NETGEAR DDNS server, you can type <code>ftp://MyName.mynetgear.com</code> to access the USB device over the Internet and download or upload files.

- Click the **Apply** button.

Your settings are saved.

Enable FTP Access Within Your Network

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

Note: For information about using FTP to access a storage device over the Internet, see *Chapter 10, Access Storage Devices Through the Internet*.

➤ **To enable FTP access within your network:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > USB Storage > Advanced Settings**.

The screenshot shows the 'ADVANCED' settings page for 'USB Storage (Advanced Settings)'. The 'Network/Device Name' is 'readystore' and the 'Workgroup' is 'Workgroup'. There are 'Apply' and 'Refresh' buttons. Below is a table of network connections:

Enable	Access Method	Link	Port
<input checked="" type="checkbox"/>	Network Connection	\\readystore	-
<input checked="" type="checkbox"/>	HTTP	http://readystore.routerlogin.net/shares	80
<input type="checkbox"/>	HTTPS (via internet)	https://0.0.0.0/shares	443
<input type="checkbox"/>	FTP	ftp://readystore.routerlogin.net/shares	21
<input type="checkbox"/>	FTP (via internet)	ftp://0.0.0.0/shares	21

Below the table is the 'Available Network Folders' section:

	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
<input checked="" type="radio"/>	\\readystore\USB_Storage	All - no password	All - no password	U:\	STORE N GO	3.72 G	617 M

Buttons for 'Edit', 'Create Network Folder', and 'Delete' are visible. At the bottom, there is a 'Safely Remove USB Device' button.

The previous figure shows a USB device attached to the modem router.

6. Select the **FTP** check box.

- Click the **Apply** button.

Your settings are saved.

View Network Folders on a Device

You can view or change the network folders on a USB storage device connected to the modem router.

➤ To view network folders:

- Launch an Internet browser from a computer or WiFi device that is connected to the network.
- Type **http://www.routerlogin.net**.
A login window opens.
- Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
- Click the **OK** button.
The BASIC Home page displays.
- Select **ADVANCED > USB Storage > Advanced Settings**.

The screenshot shows the 'ADVANCED' settings page for 'USB Storage (Advanced Settings)'. The left sidebar includes 'ADVANCED Home', 'WPS Wizard', 'Setup', 'USB Storage', 'Basic Settings', 'Advanced Settings' (selected), 'Media Server', 'Security', 'Administration', and 'Advanced Setup'. The main content area has 'Apply' and 'Refresh' buttons. Below are input fields for 'Network/Device Name' (readystore) and 'Workgroup' (Workgroup). A table lists access methods and their links/ports:

Enable	Access Method	Link	Port
<input checked="" type="checkbox"/>	Network Connection	\\readystore	-
<input checked="" type="checkbox"/>	HTTP	http://readystore.routerlogin.net/shares	80
<input type="checkbox"/>	HTTPS (via internet)	https://0.0.0.0/shares	443
<input type="checkbox"/>	FTP	ftp://readystore.routerlogin.net/shares	21
<input type="checkbox"/>	FTP (via internet)	ftp://0.0.0.0/shares	21

Below this is the 'Available Network Folders' table:

	Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
<input type="radio"/>	\\readystore\USB_Storage	All - no password	All - no password	U:\	STORE N GO	3.72 G	617 M

Buttons at the bottom include 'Edit', 'Create Network Folder', 'Delete', and 'Safely Remove USB Device'.

The previous figure shows a USB device attached to the modem router.

- In the Available Network Folders table, select a device.

If only one device is connected, it is automatically selected.

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

The Available Network Folders table shows the following settings:

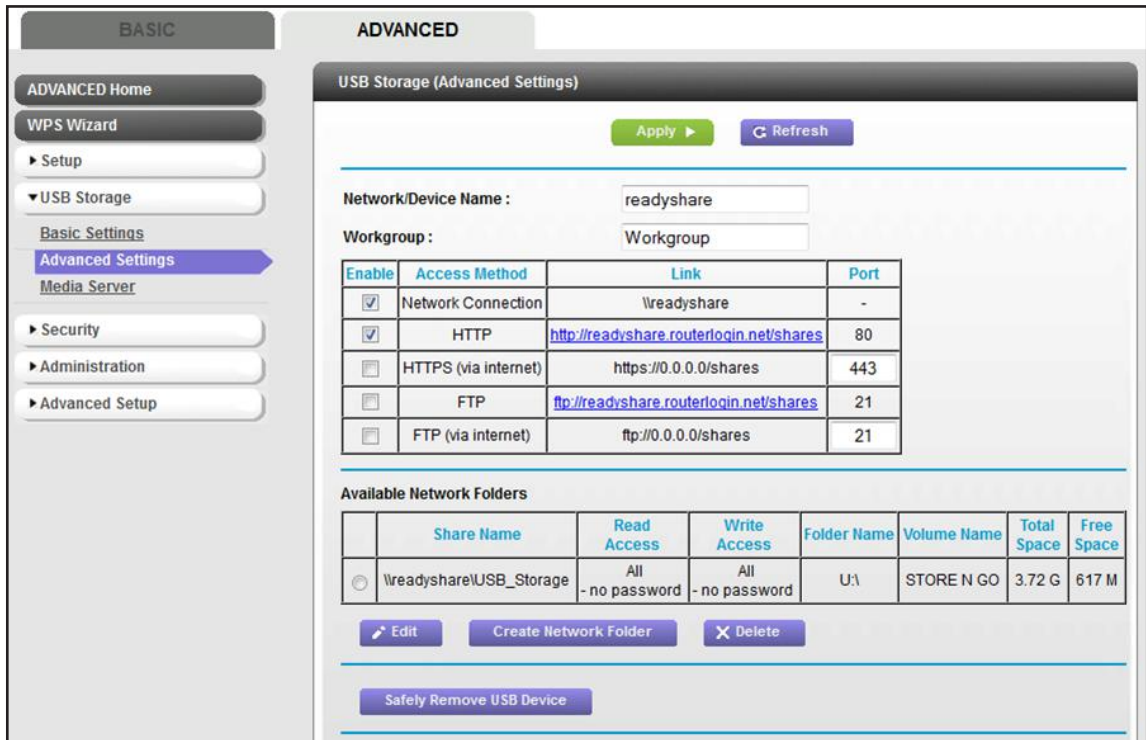
- **Share Name.** The default share name is USB_Storage.
- **Read Access and Write Access.** The permissions and access controls on the network folder. All—no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the modem router.
- **Folder Name.** Full path of the network folder.
- **Volume Name.** Volume name from the storage device.
- **Total Space and Free Space.** The current utilization of the storage device.

Add a Network Folder on a Storage Device

You can add network folders on a storage device that is connected to a USB port on the modem router.

➤ **To add a network folder:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > USB Storage > Advanced Settings**.



The previous figure shows a USB device attached to the modem router.

- In the Available Network Folders table, select a device.

If only one device is connected, it is automatically selected.

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

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

Create Network Folder

USB Device	U: (STORE N GO) ▾
Folder	U: <input type="text"/> Browse
Share Name	<input type="text"/>
Read Access	All - no password ▾
Write Access	All - no password ▾

Apply

Close Window

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

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 modem router.

11. Click the **Apply** button.

The folder is added on the storage device.

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

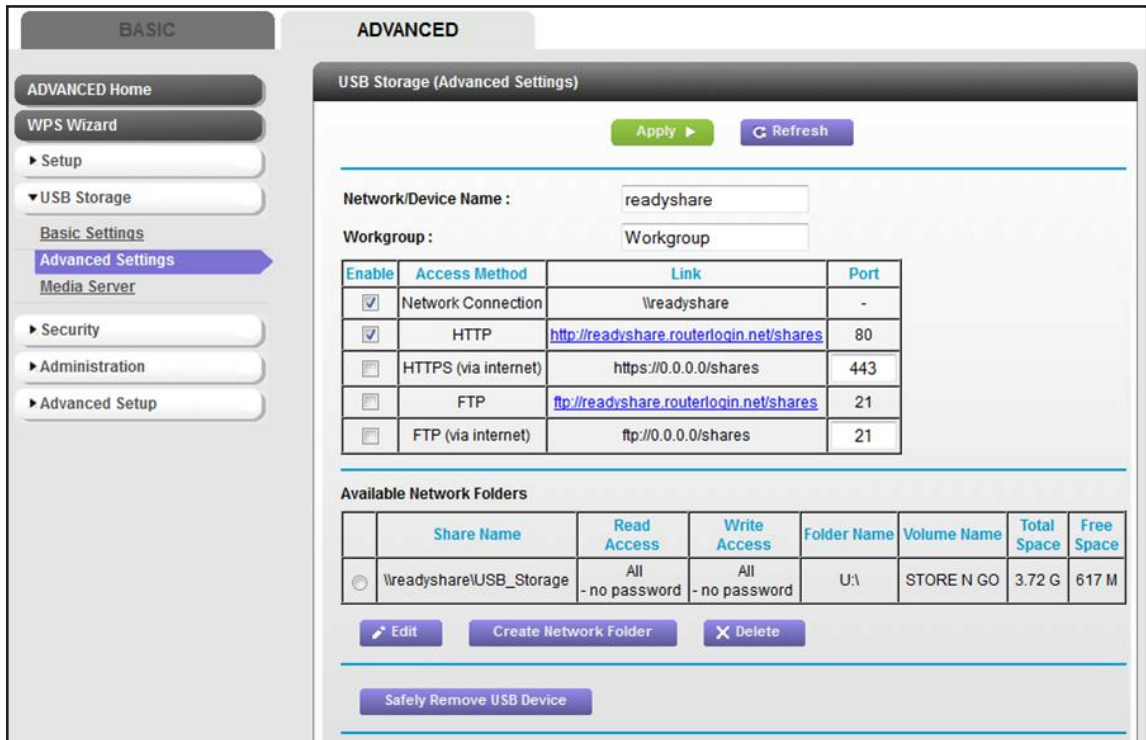
The USB Storage (Advanced Settings) page displays again.

Change a Network Folder, Including Read and Write Access, on a USB Drive

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

➤ To edit a network folder:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > USB Storage > Advanced Settings**.

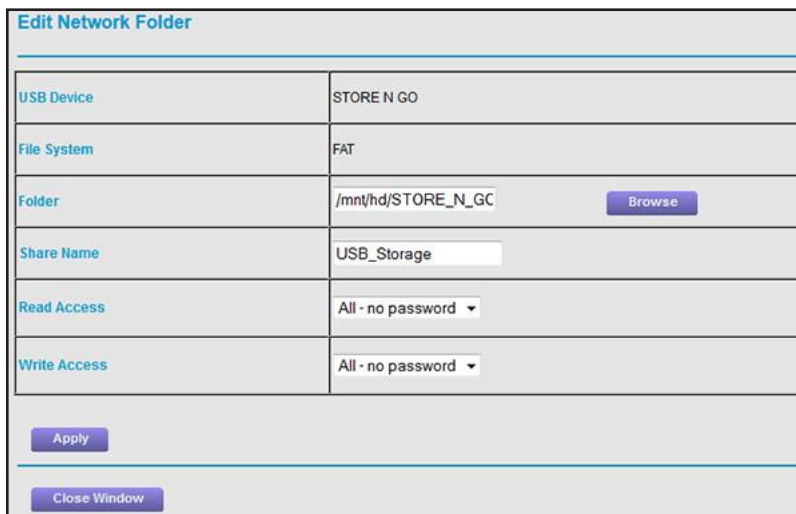


The previous figure shows a USB device attached to the modem router.

- In the Available Network Folders table, select a device.
If only one device is connected, it is automatically selected.

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

- Click the **Edit** button.



- Change the settings in the fields as needed.

For more information about the settings, see [Add a Network Folder on a Storage Device](#) on page 130.

9. Click the **Apply** button.

Your settings are saved.

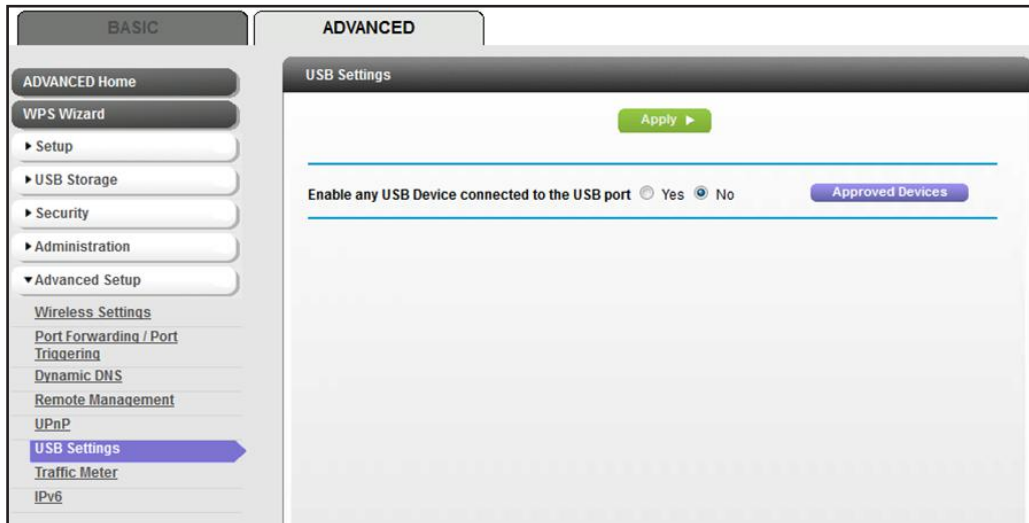
10. Click the **Close Window** button.

The USB Storage (Advanced Settings) page displays again.

Approve USB Devices

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

- **To allow only approved USB devices to connect to the modem router and specify which USB devices are approved:**
 1. Make sure that the USB device that you want to approve is attached to the modem router.
 2. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 3. Type **http://www.routerlogin.net**.
A login window opens.
 4. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 5. Click the **OK** button.
The BASIC Home page displays.
 6. Select **ADVANCED > Advanced Setup > USB Settings**.



7. Select the **No** radio button.

By default the **Yes** radio button is selected. This setting lets you connect and access all your USB devices.

8. Click the **Apply** button.

Your settings are saved.

9. Click the **Approved Devices** button.

Apply Refresh

Allow only approved devices

Approved USB Devices

	Volume Name	Device Name	Capacity

Delete

Available USB Devices

	Volume Name	Device Name	Capacity
<input type="radio"/>	STORE N GO	Verbatim STORE N GO	3.72 G

Add

10. In the Available USB Devices table, select the USB device that you want to approve.

11. Click the **Add** button.

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

12. Select the **Allow only approved devices** check box.

13. Click the **Apply** button.

Your settings are saved.

To approve another USB device that is not connected to the USB port, first remove the USB device that is connected (see [Safely Remove a USB Device](#) on page 135), connect the other USB device, and repeat this procedure.

Safely Remove a USB Device

Before you physically disconnect a USB device from the USB port on the modem router, log in to the modem router, and take the drive offline (that is, unmount the drive).

➤ To remove one or more USB devices safely:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

The BASIC Home page displays.

5. Select **ReadySHARE > Basic Settings**.

The USB Storage (Basic Settings) page displays.

6. Click the **Safely Remove USB Device** button.

The device goes offline and a pop-up window displays.

7. Click the **OK** button.

8. Physically disconnect the USB device or devices.

Enable the Media Server

The modem router can function as a ReadyDLNA media server, which lets you view movies and photos on DLNA/UPnP AV-compliant media players, such as Xbox360, Playstation, and NETGEAR media players.

- **To enable the media server, specify its settings, and scan for media content:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.

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

A login window opens.

3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

The BASIC Home page displays.

5. Select **ADVANCED > USB Storage > Media Server**.

The screenshot shows the router's web interface. On the left is a navigation menu with 'BASIC' and 'ADVANCED' tabs. Under 'ADVANCED', 'Media Server' is selected. The main content area is titled 'Media Server (Settings)'. It features a green 'Apply' button at the top right. Below it, the 'Enable Media Server' checkbox is checked. The 'Media Server Name' field contains 'ReadyDLNA' and the address ':C6250-100NAS'. Under the 'Content Scan' section, the 'Automatic (when new files added)' radio button is selected.

6. To enable the modem router to function as a media server, select the **Enable Media Server** check box.
7. In the **Media Server Name** field, specify the name of the media server.

By default, the name is ReadyDLNA:C6250-100NAS. The suffix :C6250-100NAS is added to any name that you specify. That is, if you specify the name as MyMedia, the complete name of the media server becomes MyMedia:C6250-100NAS.

Note: By default, the **Automatic (when new files added)** check box is selected to enable the modem router to scan for content when new files are added. You cannot clear this radio button.

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

9 Share a USB Printer

9

The ReadySHARE Printer utility lets you share a USB printer that is connected to a USB port on your modem router. You can share this USB printer among the Windows and Mac computers on your network.

The chapter includes the following sections:

- *Install the Printer Driver and Cable the Printer*
- *Download the ReadySHARE Printer Utility*
- *Install the ReadySHARE Printer Utility*
- *Use the Shared Printer*
- *View or Change the Status of a Printer*
- *Use the Scan Feature of a Multifunction USB Printer*
- *Change NETGEAR USB Control Center Settings*

Install the Printer Driver and Cable the Printer

Some USB printer manufacturers (for example, HP and Lexmark) request that you do not connect the USB cable until the installation software prompts you to do so.

➤ **To install the driver and cable the printer:**

1. On each computer on your network that shares the USB printer, install the driver software for the USB printer.

If the printer driver is not installed, contact the printer manufacturer.

2. Use a USB printer cable to connect the USB printer to one of the USB ports on the modem router.

Download the ReadySHARE Printer Utility

The utility works on Windows computers, Mac computers, smartphones, and tablets.

➤ **To download the ReadySHARE Printer utility:**

1. Visit netgear.com/readyshare.
2. Scroll down to the Print From the Comfort of Your Home Network section at the bottom of the page.
3. Click one of the following links:
 - **Download PC installer and get started.** This is the utility for Windows computers.
 - **Download Mac installer and get started.** This is the utility for MAC computers.
 - **Download the genie App and get started.** This is the utility for smartphones and tablets.
4. Follow the onscreen instructions to download the ReadySHARE Printer utility setup file.

Install the ReadySHARE Printer Utility

You must install the ReadySHARE Printer utility on each computer that will share the printer. After you install it, the utility displays as NETGEAR USB Control Center on your computer.

➤ **To install the utility:**

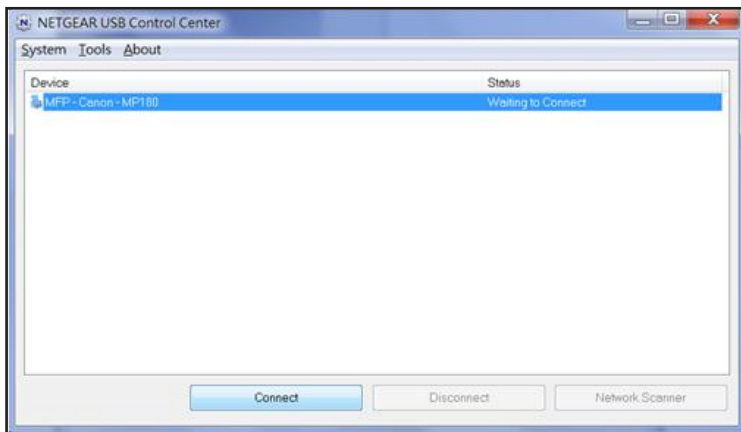
1. If necessary, unzip the ReadySHARE Printer utility setup file.
2. Double-click the ReadySHARE Printer utility setup file that you downloaded.



3. Follow the wizard instructions to install NETGEAR USB Control Center. After the InstallShield Wizard completes the installation, the NETGEAR USB Control Center prompts you to select a language.



4. Select a language from the menu and click the **OK** button.



Some firewall software, such as Comodo, blocks NETGEAR USB Control Center from accessing the USB printer. If you do not see the USB printer displayed on the page, you can disable the firewall temporarily to allow the utility to work.

5. Select the printer and click the **Connect** button.

The printer status changes to Manually connected by *Mycomputer*. Now only your computer can use the printer.

6. Click the **Disconnect** button.

The status changes to Available. Now all computers on the network can use the printer.

7. To exit the utility, select **System > Exit**.

Use the Shared Printer

For each computer, after you click the **Connect** and **Disconnect** buttons once, the utility automatically manages the printing queue. By default, the utility starts automatically whenever you log on to Windows and runs in the background.

➤ To manually connect and print:

1. Click the **NETGEAR USB Control Center** icon .

The main page displays.

2. Click the **Connect** button.

The printer status changes to Manually connected by *Mycomputer*. Now only the computer you are using can use this printer.

3. Use the print feature in your application to print your document.
4. To release the printer so that all computers on the network can use it, click the **Disconnect** button.

➤ To print and release the printer to any computer on the network:

1. To print your document, use the print feature in your application.

The NETGEAR USB Control Center automatically connects your computer to the USB printer and prints the document. If another computer is already connected to the printer, your print job goes into a queue to wait to be printed.

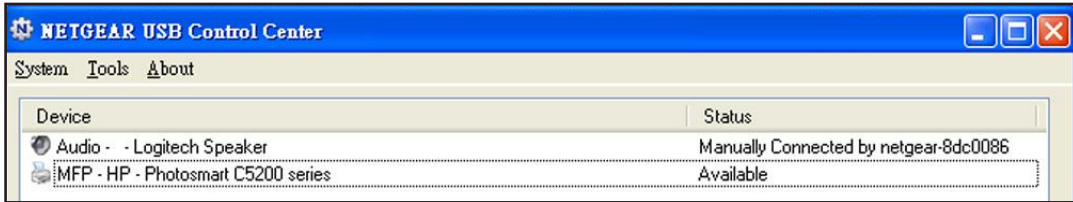
2. If your document does not print, use the NETGEAR USB Control Center to check the status.

See [View or Change the Status of a Printer](#) on page 142.

View or Change the Status of a Printer

➤ To view or change the status:

1. Click the **NETGEAR USB Control Center** icon .



The Status column shows the status for each device:

- **Available.** No print jobs are in progress. You can use the USB printer from any computer in the network.
 - **Connected.** Your computer is connected to the printer and will be released when your print job is done.
 - **Manually Connected by.** Only the connected computer can use the printer.
 - **Waiting to Connect.** Your computer is not connected to the shared printer yet.
2. To print from your computer when the status shows Manually connected by *another computer*, click the **Disconnect** button.

The printer is released from the connection and the status changes to Available.

3. To print from your computer when the status shows Waiting to Connect, do the following:
 - a. Click the **Connect** button.

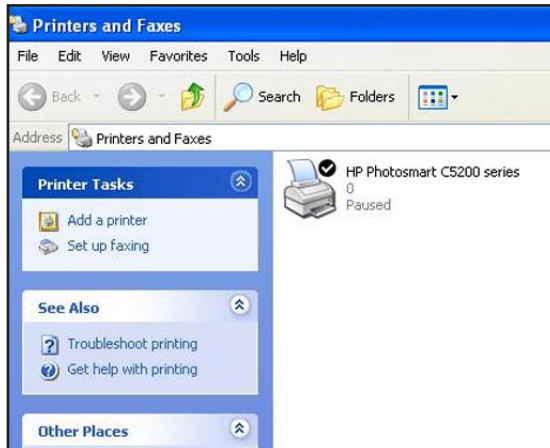
The printer status changes to Manually connected by *Mycomputer*. Now only your computer can use the printer.

- b. To allow the printer to be shared, click the **Disconnect** button.

The printer is released from the connection and the status changes to Available.

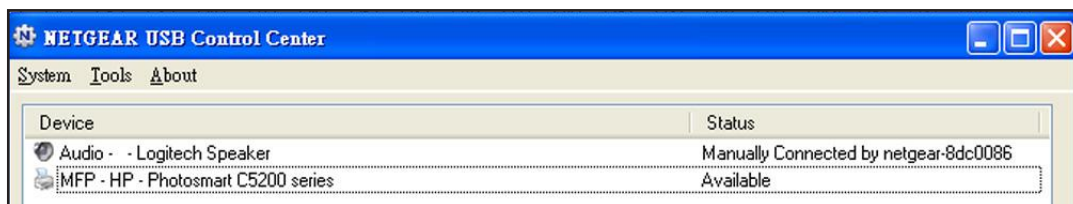
Use the Scan Feature of a Multifunction USB Printer

If your USB printer supports scanning, you can also use the USB printer for scanning. For example, the USB printer displayed in the Windows Printers and Faxes page is ready for print jobs.

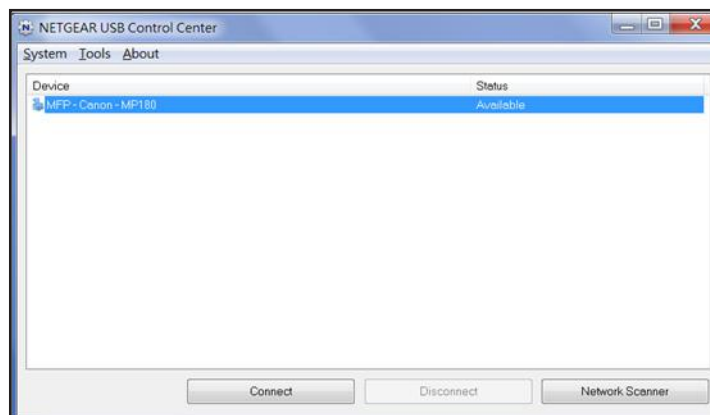


➤ To use the scan feature of a multifunction USB printer:

1. Click the **NETGEAR USB Control Center** icon .



2. Make sure that the printer status shows as Available.



3. Click the **Network Scanner** button.

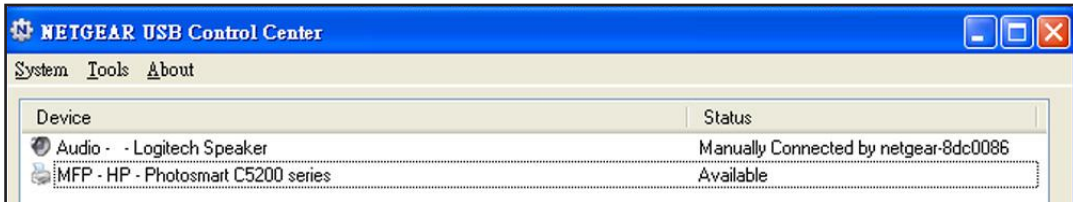
The scanner page displays so that you can use the USB printer for scanning.

Change NETGEAR USB Control Center Settings

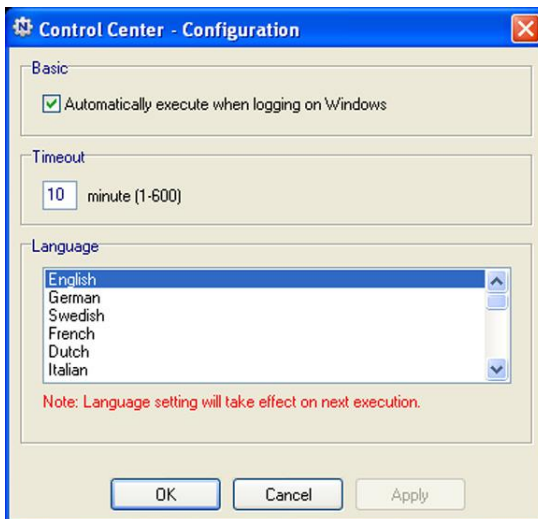
You can stop the NETGEAR USB Control Center from starting automatically when you log in to Windows. You can also change the language and specify the time-out to release the printer connection.

➤ **To turn off automatic NETGEAR USB Control Center startup:**

1. Click the **NETGEAR USB Control Center** icon .



2. Select **Tools > Configuration**.



3. Clear the **Automatically execute when logging on Windows** check box.
4. Click the **OK** button.

Your settings are saved.

Change the NETGEAR USB Control Center Language

➤ **To change the language:**

1. Click the **NETGEAR USB Control Center** icon .

The main page displays.

2. Select **Tools > Configuration**.

The Control Center - Configuration page displays.

3. From the **Language** menu, select a language.

4. Click the **OK** button.

The next time NETGEAR USB Control Center starts, the language changes.

Specify the Time-Out

➤ **To specify the time-out:**

1. Click the **NETGEAR USB Control Center** icon .

The main page displays.

2. Select **Tools > Configuration**.

The Control Center - Configuration page displays.

3. In the **Timeout** field, type the number of minutes.

The time-out is the number of minutes that a computer holds its connection to the printer when the connection is not being used.

4. Click the **OK** button.

Your settings are saved.

Access Storage Devices Through the Internet

10

With Dynamic DNS, you can use the Internet and a personal domain name to access a USB storage device that is attached to a USB port on the modem router when you are not home. If you know the IP address of the modem router (and the IP address did not change), you can also access the USB storage device by using the IP address.

This chapter includes the following sections:

- *Set Up and Manage Dynamic DNS*
- *Access Storage Devices Through the Internet*

Note: For information about how to connect the device and specify its settings, see *Chapter 8, Share a Storage Device*.

Set Up and Manage Dynamic DNS

Internet service providers (ISPs) assign numbers called IP addresses to identify each Internet account. Most ISPs use dynamically assigned IP addresses. This means that the IP address can change at any time. You can use the IP address to access your network remotely, but most people do not know what their IP addresses are or when these numbers change.

To make it easier to connect, you can get a free account with a Dynamic DNS service that lets you use a domain name to access your home network. To use this account, you must set up the modem router to use Dynamic DNS. Then the modem router notifies the Dynamic DNS service provider whenever its IP address changes. When you access your Dynamic DNS account, the service finds the current IP address of your home network and automatically connects you.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

Your Personal FTP Server

With your customized free URL, you can use FTP to access your network when you are not home through Dynamic DNS. To set up your FTP server, you must register for a NETGEAR Dynamic DNS (DDNS) service account and specify the account settings (see [Set Up a New Dynamic DNS Account](#) on page 148).

➤ To set up your personal account and use FTP:

1. Get your NETGEAR Dynamic DNS domain name.

For more information, see [Set Up a New Dynamic DNS Account](#) on page 148.

2. Make sure that your Internet connection is working.

Your modem router must use a direct Internet connection. It cannot connect to a different router to access the Internet.

3. Connect a USB storage device to the USB port on the modem router.
4. If your USB device uses a power supply, connect it.

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

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

5. Set up FTP access on the modem router.

For more information, see [Set Up FTP Access Through the Internet](#) on page 151.

6. On a remote computer with Internet access, you can use FTP to access your modem router using `ftp://yourname.mynetgear.com`, in which *yourname* is your specific domain name.

For more information, see [Access Storage Devices Through the Internet with FTP](#) on page 153.

Set Up a New Dynamic DNS Account

NETGEAR offers you the opportunity to set up and register for a free Dynamic DNS account.

- **To set up Dynamic DNS and register for a free NETGEAR account:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.
 5. Select **ADVANCED > Advanced Setup > Dynamic DNS**.

6. Select the **Use a Dynamic DNS Service** check box.
7. From the **Service Provider** menu, select **NETGEAR**.

powered by no-ip

Use a Dynamic DNS Service

Service Provider: NETGEAR

Do you have a NETGEAR DDNS or a No-IP DDNS account?

Yes

No

Please enter the following information for registration.

Host Name: _____ .mynetgear.com

Email: _____

Password (6~32 characters): _____

By submitting this form I agree to the [terms of service](#) and that I will only create one free account.

8. Select the **No** radio button.
9. In the **Host Name** field, enter 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*.
10. In the **Email** field, enter the email address that you want to use for your account.
11. In the **Password (6-32 characters)** field, enter the password that you want to use for your account.
12. Click the **Register** button.
13. 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, Dyn (also referred to as DynDNS), or DtDNS, you can set up the modem router to use your account.

- **To set up Dynamic DNS if you already created an account:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
 4. Click the **OK** button.
The BASIC Home page displays.

5. Select **ADVANCED > Advanced Settings > Dynamic DNS**.

6. Select the **Use a Dynamic DNS Service** check box.
7. From the **Service Provider** menu, select your provider.
8. Select the **Yes** radio button.
- The page adjusts.
9. In the **Host Name** field, enter the host name (sometimes called the domain name) for your account.
10. Depending on the type of account, specify your user name or email address:
- For a No-IP, Dyn, or DtDNS account, in the **User Name** field, enter the user name for your account.
 - For a NETGEAR account, in the **Email** field, enter the email address for your account.
11. In the **Password** field, enter the password for your DDNS account.
12. Click the **Apply** button.

Your settings are saved.

13. To verify that your Dynamic DNS service is enabled in the modem router, click the **Show Status** button.

A message displays the Dynamic DNS status.

Access Storage Devices Through the Internet

If you connect a USB storage device to the modem router, you can access the USB device through the Internet when you are not home. After you gain access, you can use FTP to share files on the USB device.

➤ To access devices from a remote computer:

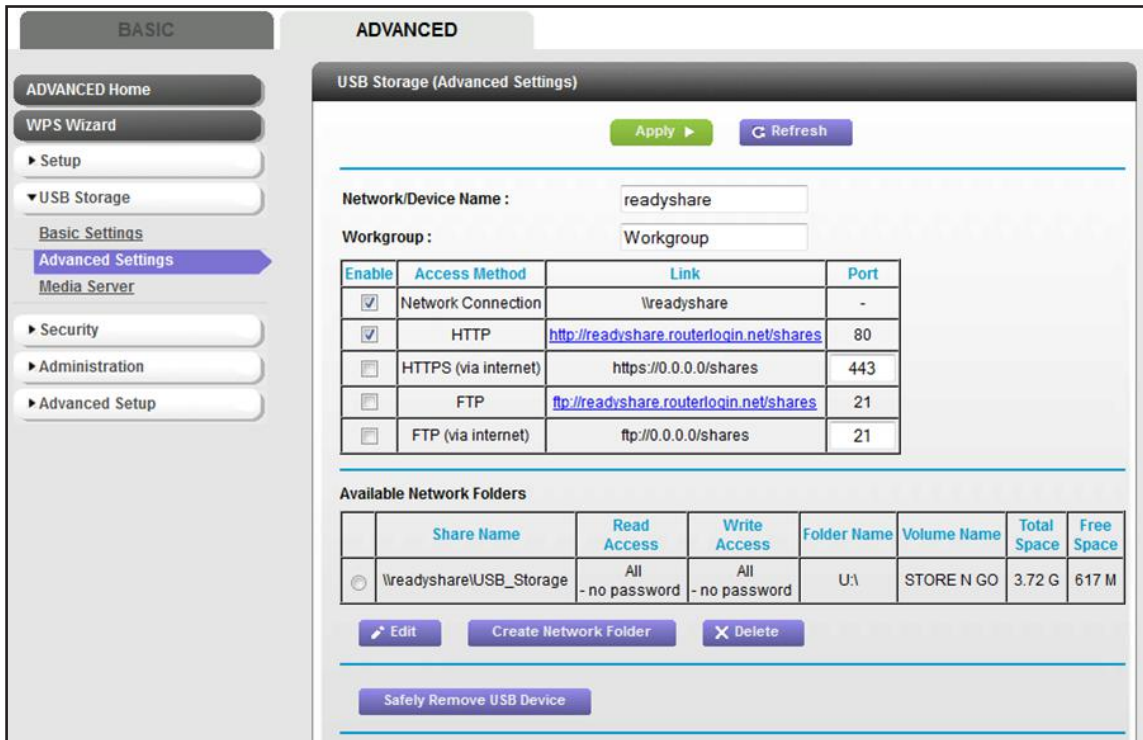
1. Launch a web browser on a computer that is not on your home network.
2. Connect to your modem router on your home network:
 - To connect with Dynamic DNS, type the DNS name.
To use a Dynamic DNS account, you must enter the account information in the Dynamic DNS page (see *Set Up and Manage Dynamic DNS* on page 147).
 - To connect without Dynamic DNS, type the modem router's Internet port IP address.
You can view the modem router's Internet IP address on the BASIC Home page.

Set Up FTP Access Through the Internet

If you attach a storage device to the modem router, you can access the storage device from your network (see *Enable FTP Access Within Your Network* on page 128). You can also set up FTP access through the Internet so that you can access the storage device from outside your local network, for example, when you are not at home.

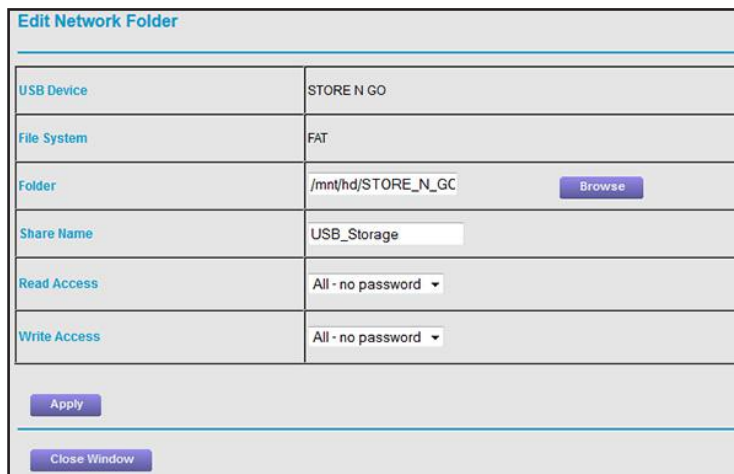
➤ To set up FTP access through the Internet:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > USB Storage > Advanced Settings**.



The previous figure shows a USB device attached to the modem router.

6. Select the **FTP (via Internet)** check box.
7. Click the **Apply** button.
Your settings are saved.
8. To limit access to the admin user, do the following:
 - a. In the Available Network Folders table, select a device.
If only one device is connected, it is automatically selected.
 - b. Click the **Edit** button.



- c. In the **Read Access** list, select **admin**.
- d. In the **Write Access** list, select **admin**.
- e. Click the **Apply** button.

Your settings are saved.

- f. Click the **Close Window** button.

The USB Storage (Advanced Settings) page displays again.

Access Storage Devices Through the Internet with FTP

If you attached a storage device to the modem router, before you can access the storage device through the Internet with FTP, you must first set it up (see *Set Up FTP Access Through the Internet* on page 151).

- **To access a USB device with FTP from a remote computer to download or upload a file:**

1. Take one of the following actions:

- To download a file from a storage device connected to the modem router, launch a web browser.
- To upload a file to a storage device connected to the modem router, launch an FTP client such as Filezilla.

2. In the address field of the browser, type **ftp://** and the Internet port IP address.

For example, if your IP address is 10.1.65.4, type **ftp://10.1.65.4**.

If you are using Dynamic DNS, type the DNS name.

For example, type **ftp://MyName.mynetgear.com**.

3. When prompted, log in:

- To log in as admin, in the **user name** field, enter **admin** and in the **password** field, enter the same password that you use to log in to the modem router.
- To log in as guest, in the **user name** field, enter **guest**.

The guest user name does not need a password.

The files and folders that your account can access on the USB device display. For example, you might see `share/partition1/directory1`.

4. Navigate to a location on the USB device.
5. Download or upload the file.

Manage the Advanced WiFi Network Settings

11

This chapter describes how to configure the advanced WiFi settings.

This chapter contains the following sections:

- *Control the WiFi Radios*
- *Set Up a WiFi Schedule*
- *Manage Beamforming*
- *Manage the Advanced WiFi Settings*
- *Manage WPS Settings*
- *Manage the Advanced WiFi Features*

Note: For information about the managing the basic WiFi settings, see *Chapter 4, Manage the Basic WiFi Network Settings*.

Control the WiFi Radios

The modem router provides internal WiFi radios that 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 modem router. When the WiFi radios are off, you can still use an Ethernet cable for a LAN connection to the modem router.

You can turn the WiFi radios on and off with the **WiFi On/Off** button on the modem router, or you can log in to the modem router and enable or disable the WiFi radios through the web management interface. If you are close to the modem router, it might be easier to press the **WiFi On/Off** button. If you are away from the modem router or already logged in, it might be easier to enable or disable the radios through the web management interface. You can also turn the WiFi radios off and on based on a schedule. (See *Set Up a WiFi Schedule* on page 156.)

Tip: If you want to disable the WiFi radios of the modem router, use a wired connection to avoid being disconnected when the WiFi radios turn off.

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 right side panel of the modem router for three seconds.

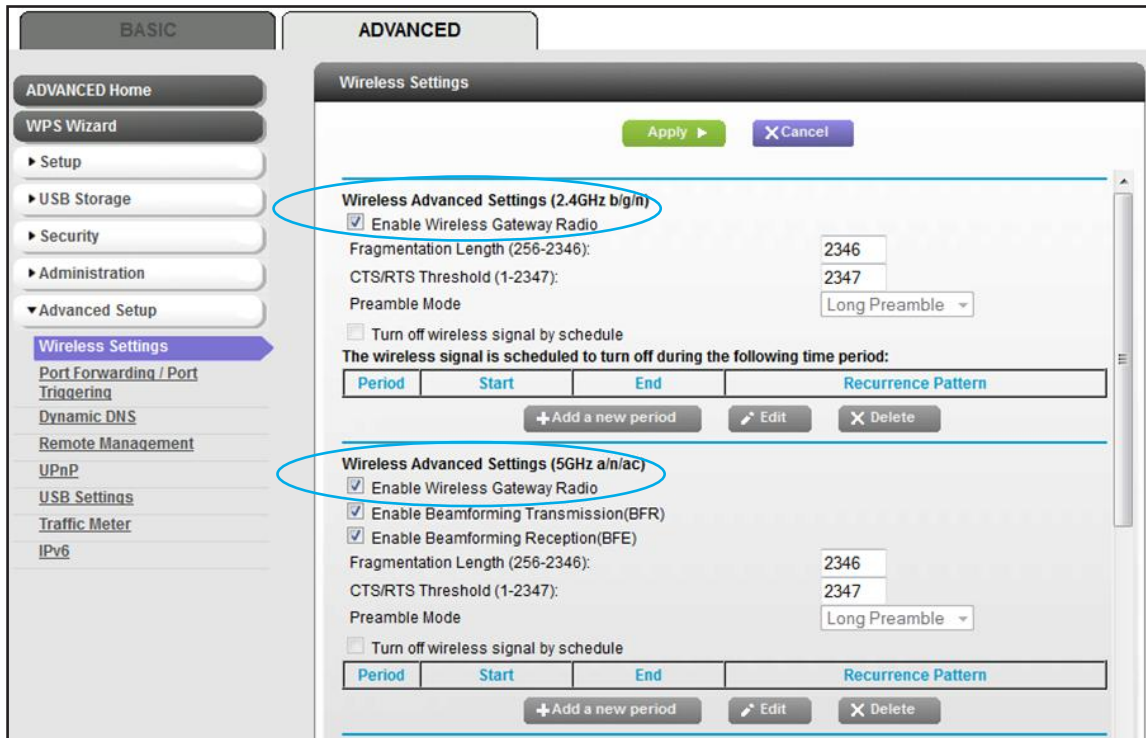
If you turned off the WiFi radios, the 2.4 GHz WiFi LED and 5 GHz WiFi LED turn off. If you turned on the WiFi radios, these WiFi LEDs lights solid green.

Enable or Disable the WiFi Radios

If you used the **WiFi On/Off** button to turn off the WiFi radios, you cannot log in to the modem router over a WiFi connection to turn them back on. You must press the **WiFi On/Off** button again for three seconds to turn the WiFi radios back on.

➤ To enable or disable the WiFi radios:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Wireless Settings**.



The previous figure does not show the bottom of the Wireless Settings page.

6. Do one of the following in the Wireless Advanced Settings (2.4GHz b/g/n) section, Wireless Advanced Settings (5GHz 802.11a/n/ac) section, or both sections:
 - **Turn off the radio.** Clear the **Enable Wireless Router Radio** check box.
The WiFi LED for the associated radio turns off (see *Front Panel and Right Side Panel* on page 10).
 - **Turn on the radio.** Select the **Enable Wireless Router Radio** check box.
The WiFi LED for the associated radio lights solid green.
7. Click the **Apply** button.
Your settings are saved.

Set Up a WiFi Schedule

You can use this feature to turn off the WiFi signal from your modem router at times when you do not need a WiFi connection. For example, you might turn it off for the weekend if you leave town. You can set up separate schedules for the 2.4 GHz and 5 GHz bands.

Note: You can set up a WiFi schedule only if the modem router is connected to the Internet and synchronized its internal clock with a time server on the Internet. For more information about whether the modem router synchronized its clock, see *Schedule When Security Features Are Active* on page 75.

➤ **To set up the WiFi schedule:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type <http://www.routerlogin.net>.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Wireless Settings**.

The previous figure does not show the bottom of the Wireless Settings page.

6. Either in Wireless the Advanced Settings (2.4GHz b/g/n) section or the Wireless Advanced Settings (5GHz 802.11a/n/ac) section, click the **Add a new period** button.

The Turn off wireless signal by schedule page displays.

7. Use the menus, radio buttons, and check boxes to set up a period during which you want to turn off the WiFi signal and specify whether the schedule is recurrent.
8. Click the **Apply** button.

The Wireless Settings page displays. Depending on the WiFi band for which you set up a schedule, the new schedule is added to the table in the Wireless Advanced Settings (2.4GHz b/g/n) section or the Wireless Advanced Settings (5GHz 802.11a/n/ac) section.

9. Select the **Turn off wireless signal by schedule** check box to activate the schedule.
10. Click the **Apply** button.

Your settings are saved.

Manage Beamforming

The modem router supports beamforming in the 5 GHz band to enhance the WiFi range and performance for your a/n/ac WiFi devices. When you enable beamforming and connect to the WiFi network, the modem router actively tracks your device and directs WiFi to your device, rather than just blasting it out in all directions. Beamforming provides a better range and performance and is enabled by default. You can manage beamforming transmission (BFR) from the modem router to the WiFi clients and beamforming reception (BFE) from the WiFi clients to the modem router by turning it on or off.

➤ To enable or disable beamforming:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Wireless Settings**.

6. Select or clear the **Enable Beamforming Transmission (BFR)** check box.
Selecting the check box enables BFR and clearing the check box disables BFR.
7. Select or clear the **Enable Beamforming Reception (BFE)** check box.
Selecting the check box enables BFE and clearing the check box disables BFE.
8. Click the **Apply** button.
Your settings are saved.

Manage the Advanced WiFi Settings

The modem router is already configured with the optimum settings. Do not change the advanced WiFi settings (fragmentation length and CTS/RTS threshold) unless directed by technical support. Incorrect settings might disable the WiFi radios.

- **To change the advanced WiFi settings:**
 1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
 2. Type **http://www.routerlogin.net**.
A login window opens.
 3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.

- Click the **OK** button.
The BASIC Home page displays.
- Select **ADVANCED > Advanced Setup > Wireless Settings**.



CAUTION:

Do not alter the advanced WiFi settings unless directed by technical support. These settings are reserved for WiFi testing and advanced configuration only. Incorrect settings might disable the WiFi radios.

- Change the advanced WiFi settings for one radio or both radios:
 - Fragmentation Length (256-2346)**. The default setting is 2346.
 - CTS/RTS Threshold (1-2347)**. The default setting is 2347.

You can change these settings both in the Wireless Advanced Settings (2.4GHz b/g/n) section and in the Wireless Advanced Settings (5GHz 802.11a/n/ac) section.

The selection from the **Preamble Mode** menu is fixed at **Long Preamble**.

- If you changed the settings, click the **Apply** button.
Your settings are saved.

Manage WPS Settings

You can control how WPS functions on the modem router. Use caution if you change the WPS settings.

Note: For information about how to use WPS to add WiFi devices and other equipment to your WiFi network, see *Join the WiFi Network of the Modem Router* on page 21 and *Use the WPS Wizard to Add a Device to the WiFi Network* on page 45.

➤ **To specify WPS settings:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Wireless Settings**.
The Wireless Settings page displays.
6. Scroll down to the WSP Settings section.



WPS Settings	
Gateway's PIN:	18476231
<input type="checkbox"/> Disable Gateway's PIN	
<input checked="" type="checkbox"/> Keep Existing Wireless Settings (2.4GHz b/g/n)	
<input checked="" type="checkbox"/> Keep Existing Wireless Settings (5GHz a/n/ac)	

The **Gateway's PIN** field displays the PIN that you can enter on a registrar (for example, Windows Connect Now in Microsoft Windows 7) to configure the modem router's WiFi settings through WPS.

7. Specify the WPS settings:
 - **Disable Gateway's PIN.** By default, the PIN is enabled, but situations might occur in which you want to disable the PIN. The PIN function might temporarily be disabled when the modem router detects suspicious attempts to break into the modem router's WiFi settings through use of the modem router's PIN and WPS. You can manually disable the PIN function by selecting the **Disable Router's PIN** check box.

- **Keep Existing Wireless Settings.** By default, the **Keep Existing Wireless Settings** check boxes are selected for the 2.4 GHz and 5 GHz bands.

NETGEAR recommends that you leave these check boxes selected. However, when these check boxes are selected, some applications might not detect the modem router.



CAUTION:

When you clear a **Keep Existing Wireless Settings** check box and you add a new WiFi client through WPS, the modem router's WiFi settings for the associated network change to an automatically generated SSID and passphrase (also referred to as the WiFi network password or network key).

8. Click the **Apply** button.

Your settings are saved.

Manage the Advanced WiFi Features

The modem router supports the following advanced WiFi features:

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

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

- **PMF.** Protected Management Frames (PMF) is a security feature that protects unicast and multicast management frames from being intercepted and changed for malicious purposes. This feature is disabled by default, but you can enable it.

PMF is supported in Windows 8. If all computers on your network run Windows 8, you can enable PMF. If you are not sure, keep PMF disabled.

- **WMF.** Wireless Multicast Forwarding (WMF) lets the modem router forward multicast frames to wireless LAN (WLAN) hosts, using unicast addresses. WMF provides robust wireless communication because unicast frames are acknowledged, retried, and dynamically rate-controlled. This feature is enabled by default, but you can disable it.
- **ATF.** Airtime Fairness (ATF) ensures that all WiFi clients receive equal time on the network. Network resources are divided by time, so if five WiFi clients are connected to the network, they each get one-fifth of the network time. The advantage of this feature is that the slowest WiFi clients do not control network responsiveness. This feature is disabled by default, but you can enable it.

➤ **To manage the advanced WiFi features:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Wireless Settings**.
The Wireless Settings page displays.
6. Scroll down to the bottom of the page.

WMM	
<input checked="" type="checkbox"/>	WMM Support (2.4GHz b/g/n)
<input checked="" type="checkbox"/>	WMM Support (5GHz a/n/ac)
PMF	
Protected Management Frames (2.4GHz b/g/n)	Off
Protected Management Frames (5GHz a/n/ac)	Off
WMMF	
<input checked="" type="checkbox"/>	Wireless Multicast Forwarding (2.4GHz b/g/n)
<input checked="" type="checkbox"/>	Wireless Multicast Forwarding (5GHz a/n/ac)
ATF	
<input type="checkbox"/>	Enable Airtime Fairness (2.4GHz b/g/n)
<input type="checkbox"/>	Enable Airtime Fairness (5GHz a/n/ac)

7. Enter the settings as described in the following table.

Field	Description
WMM	To disable WMM for the 2.4 GHz band, clear the WMM Support (2.4GHz b/g/n) check box. By default, this check box is selected and WMM is enabled for the 2.4 GHz band.
	To disable WMM for the 5 GHz band, clear the WMM Support (5GHz a/n/ac) check box. By default, this check box is selected and WMM is enabled for the 5 GHz band.

Field	Description
PFM	To enable PFM for the 2.4 GHz band, select one of the following options from the Protected Management Frames (2.4GHz b/g/n) menu: <ul style="list-style-type: none"> • Capable. The 2.4 GHz radio can receive protected management frames but does not require them. • Required. The 2.4 GHz radio requires protected management frames and rejects unprotected management frames. By default, Off is selected and PFM is disabled for the 2.4 GHz band.
	To enable PFM for the 5 GHz band, select one of the following options from the Protected Management Frames (5GHz a/n/ac) menu: <ul style="list-style-type: none"> • Capable. The 5 GHz radio can receive protected management frames but does not require them. • Required. The 5 GHz radio requires protected management frames and rejects unprotected management frames. By default, Off is selected and PFM is disabled for the 5 GHz band.
WMF	To disable WMF for the 2.4 GHz band, clear the Wireless Multicast Forwarding (2.4GHz b/g/n) check box. By default, this check box is selected and WMF is enabled for the 2.4 GHz band.
	To disable WMF for the 5 GHz band, clear the Wireless Multicast Forwarding (5GHz a/n/ac) check box. By default, this check box is selected and WMF is enabled for the 5 GHz band.
ATF	To enable ATF for the 2.4 GHz band, select the Enable Airtime Fairness (2.4GHz b/g/n) check box. By default, this check box is cleared and ATF is disabled for the 2.4 GHz band.
	To enable ATF for the 5 GHz band, select the Enable Airtime Fairness (5GHz a/n/ac) check box. By default, this check box is cleared and ATF is disabled for the 5 GHz band.

8. Click the **Apply** button.

Your settings are saved.

12 Manage Port Forwarding and Port Triggering

12

You can use outbound firewall rules, port forwarding, and port triggering to set up rules for Internet traffic for services and applications. You need networking knowledge to set up these features.

This chapter includes the following sections:

- *Manage Port Forwarding to a Local Server for Services, Applications, and Games*
- *Manage Port Triggering for Services, Applications, and Games*

Manage Port Forwarding to a Local Server for Services, Applications, and Games

If a server is part of your network, you can allow certain types of incoming traffic to reach the server. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

The modem 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 modem router forwards all other incoming protocols (see *Set Up a Default DMZ Server* on page 82).

Forward Incoming Traffic for a Default Service or Application

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

➤ **To forward incoming traffic for a default service or application:**

1. Decide which type of service, application, or game you want to provide.
2. Find the local IP address of the computer on your network that will provide the service.
The server computer must always receive the same IP address. To specify this setting, use the reserved IP address feature. See *Manage IP Address Reservation* on page 85.
3. Launch an Internet browser from a computer or WiFi device that is connected to the network.
4. Type **http://www.routerlogin.net**.
A login window opens.
5. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
6. Click the **OK** button.
The BASIC Home page displays.
7. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.

8. Make sure that the **Port Forwarding** radio button is selected.
9. From the **Service Name** menu, select the service or application.

If the service or application that you want to add is not in the menu, create a port forwarding rule with a custom service or application (see [Add a Port Forwarding Rule with a Custom Service or Application](#) on page 167).

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

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

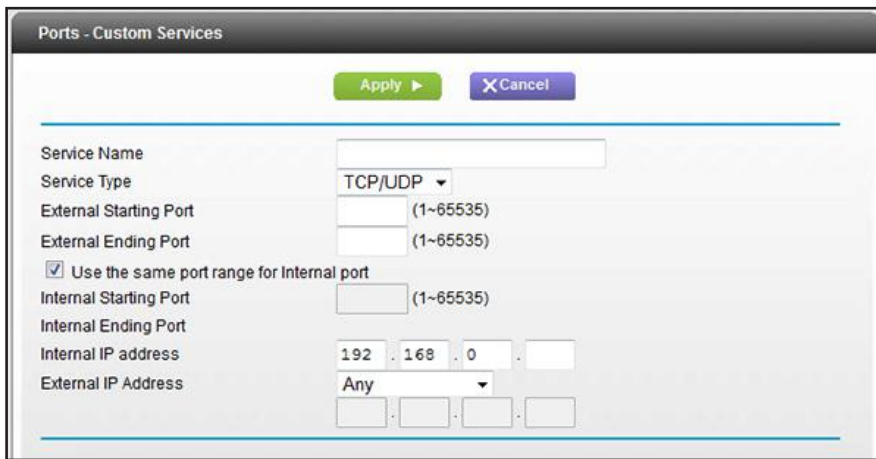
Add a Port Forwarding Rule with a Custom Service or Application

The modem 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 an Internet browser from a computer or WiFi device that is connected to the network.
 3. Type <http://www.routerlogin.net>.

A login window opens.

4. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
5. Click the **OK** button.
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. Click the **Add Custom Service** button.



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

Field	Description
Service Name	Enter the name of the custom service or application.
Service Type	Select the protocol (TCP or UDP) that is associated with the service or application. If you are unsure, select TCP/UDP .
External Starting Port	Enter the external start port number that the service or application uses.
External Ending Port	Enter the external end port number that the service or application uses.
Internal Starting Port	Specify the internal start port by one of these methods: <ul style="list-style-type: none"> • Leave the Use the same port range for Internal port check box selected. • Clear the Use the same port range for Internal port check box and enter the internal start port number that the service or application uses.
Internal Ending Port	Specify the internal end port by one of these methods: <ul style="list-style-type: none"> • Leave the Use the same port range for Internal port check box selected. • Clear the Use the same port range for Internal port check box and enter the internal end port number that the service or application uses.

Field	Description
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.
External IP address	Specify the external IP address by one of these methods: <ul style="list-style-type: none"> • Leave Any selected from the External IP address menu. • Select Single address from the External IP address menu and enter the IP address that is allowed to reach the service or application.

10. 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 an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The following figure shows two port forwarding rules.

ADVANCED

Port Forwarding / Port Triggering

Apply Cancel

Please select the service type.

Port Forwarding
 Port Triggering

Port Forwarding

Never
 Always

Service Name: FTP Server IP Address: 192 . 168 . 0 + Add

#	Enable	Service Name	External Port	External IP Address	Internal Port	Internal IP Address
1	<input checked="" type="checkbox"/>	SSH	TCP/UDP: 22	Any	TCP/UDP: 22	192.168.0.112
2	<input checked="" type="checkbox"/>	bbn-mmc	UDP: 1347	203.113.0.24	UDP: 1347	192.168.0.59

Edit Service Delete Service + Add Custom Service

6. Make sure that the **Port Forwarding** radio button is selected.
7. In the table, select the radio button next to the service or application name.
8. Click the **Edit Service** button.

The Ports - Custom Services page displays.

9. Change the settings.

For more information about the settings, see [Add a Port Forwarding Rule with a Custom Service or Application](#) on page 167.

10. 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 an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.

A login window opens.

3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

- Click the **OK** button.

The BASIC Home page displays.

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

The following figure shows two port forwarding rules.

ADVANCED

Port Forwarding / Port Triggering

Apply ▶ X Cancel

Please select the service type.

Port Forwarding
 Port Triggering

Port Forwarding

Never
 Always

Service Name: FTP Server IP Address: 192 . 168 . 0 . Add

Port Forwarding Portmap Table

#	Enable	Service Name	External Port	External IP Address	Internal Port	Internal IP Address
1	<input checked="" type="checkbox"/>	SSH	TCP/UDP: 22	Any	TCP/UDP: 22	192.168.0.112
2	<input checked="" type="checkbox"/>	bbn-mmc	UDP: 1347	203.113.0.24	UDP: 1347	192.168.0.59

Edit Service X Delete Service + Add Custom Service

- Make sure that the **Port Forwarding** radio button is selected.
- In the table, select the radio button next to the service or application name.
- Click the **Delete Service** button.

The rule is removed from the table.

Application Example: Make a Local Web Server Public

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

➤ To make a local web server public:

- Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation.

In this example, your modem router always gives your web server an IP address of 192.168.1.55.

- On the Port Forwarding / Port Triggering page, configure the modem router to forward the HTTP service to the local address of your web server at **192.168.1.55**.

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 modem router.

Dynamic DNS makes it much easier to access a server from the Internet because you can enter the name in the Internet browser. Otherwise, you must know the IP address that the ISP assigned, which typically changes.

How the Modem Router Implements the Port Forwarding Rule

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

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

Manage Port Triggering for Services, Applications, and Games

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

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

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance, enable Universal Plug and Play (UPnP). See *Manage Universal Plug and Play* on page 92.

Add a Port Triggering Rule

The modem 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 an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
6. Select the **Port Triggering** radio button.

The screenshot shows the 'ADVANCED' configuration page for 'Port Forwarding / Port Triggering'. The left sidebar lists various settings, with 'Port Forwarding / Port Triggering' highlighted. The main content area has the following settings:

- Apply** and **Cancel** buttons at the top.
- Please select the service type:**
 - Port Forwarding
 - Port Triggering
- Port Triggering:**
 - Never
 - Always
- Port Triggering Time-out (in minutes):** 10
- Port Triggering Portmap Table:**

#	Enable	Service Name	Service Type	Inbound Connection	Service User
- Buttons at the bottom: **+ Add Service**, **Edit Service**, and **Delete Service**.

7. Click the **Add Service** button.

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

Field	Description
Service Name	Enter the name of the custom service or application.
Service User	From the Service User menu, select Any , or select Single address and enter the IP address of one computer: <ul style="list-style-type: none"> Any. This is the default setting and allows any computer on the Internet to use this service. Single address. Restricts the service to a particular computer.
Service Type	Select the protocol (TCP or UDP) that is associated with the service or application.
Triggering Starting Port	Enter the number of the outbound traffic start port that must open the inbound ports.
Triggering Ending Port	Enter the number of the outbound traffic end port that must open the inbound ports.
Inbound Connection	
Starting Port	Enter the start port number for the inbound connection.
Ending Port	Enter the end port number for the inbound connection.

- Click the **Apply** button.

Your settings are saved. The rule is added to the Port Triggering Portmap Table on the Port Forwarding / Port Triggering page and is enabled.

Change a Port Triggering Rule

You can change an existing port triggering rule.

➤ To change a port triggering rule:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type <http://www.routerlogin.net>.

A login window opens.

3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

The BASIC Home page displays.

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

The Port Forwarding / Port Triggering page displays.

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

The following figure shows two port triggering rules.

The screenshot shows the 'Port Forwarding / Port Triggering' configuration page. The 'Service Type' is set to 'Port Triggering'. The 'Port Triggering' options are 'Never' (selected) and 'Always'. The 'Port Triggering Time-out (in minutes)' is set to 10. Below this is a 'Port Triggering Portmap Table' with two rows of services: 'Galaxy' and 'TomPush'. Each row has a radio button, an 'Enable' checkbox, and columns for 'Service Name', 'Service Type', 'Inbound Connection', and 'Service User'. At the bottom, there are buttons for '+ Add Service', 'Edit Service', and 'Delete Service'.

#	Enable	Service Name	Service Type	Inbound Connection	Service User
1	<input checked="" type="checkbox"/>	Galaxy	TCP: 35610 ~ 35612	TCP: 8320 ~ 8321	Any
2	<input checked="" type="checkbox"/>	TomPush	UDP: 51793 ~ 51795	UDP: 10563 ~ 10565	192.168.0.22

7. In the Port Triggering Portmap Table, select the radio button next to the service or application name.

8. Click the **Edit Service** button.

The Port Triggering - Services page displays.

9. Change the settings.

For more information about the settings, see [Add a Port Triggering Rule](#) on page 173.

10. 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.

Disable or Remove a Port Triggering Rule

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

➤ **To disable or remove a port triggering rule:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.

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

A login window opens.

3. Type **admin** for the user name and type your password.

If you did not yet personalize your password, type **password** for the password.

4. Click the **OK** button.

The BASIC Home page displays.

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

The Port Forwarding / Port Triggering page displays.

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

The following figure shows two port triggering rules.

The screenshot shows the 'ADVANCED' settings page for 'Port Forwarding / Port Triggering'. The 'Port Triggering' radio button is selected. The 'Port Triggering Time-out (in minutes)' is set to 10. The 'Port Triggering Portmap Table' contains the following data:

#	Enable	Service Name	Service Type	Inbound Connection	Service User
1	<input checked="" type="checkbox"/>	Galaxy	TCP: 35610 ~ 35612	TCP: 8320 ~ 8321	Any
2	<input checked="" type="checkbox"/>	TomPush	UDP: 51793 ~ 51795	UDP: 10563 ~ 10565	192.168.0.22

7. To disable the rule, do the following:
 - a. In the Enable column of the Port Triggering Portmap Table, clear the check box next to the service or application name.
 - b. Click the **Apply** button.
Your settings are saved.
8. To remove the rule entirely, do the following:
 - a. In the Port Triggering Portmap Table, select the radio button next to the service or application name.
 - b. Click the **Delete Service** button.
The rule is removed from the Port Triggering Portmap Table.

Specify the Time-Out Period for Port Triggering

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

➤ To specify the time-out for port triggering:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
6. Select the **Port Triggering** radio button.
The port triggering settings display.
7. In the **Port Triggering Time-out** field, enter a value up to 9999 minutes.
The default setting is 10 minutes.
8. 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 an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Advanced Setup > Port Forwarding / Port Triggering**.
The Port Forwarding / Port Triggering page displays.
6. Select the **Port Triggering** radio button.
The port triggering settings display.
7. Select the **Disable Port Triggering** check box.
If this check box is selected, the modem router does not apply port triggering rules even if you specified them.
8. Click the **Apply** button.
Your settings are saved.

Application Example: Port Triggering for Internet Relay Chat

Some application servers, such as FTP and IRC servers, send replies to multiple port numbers. Using port triggering, you can tell the modem 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 modem 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 modem router.
3. Your modem router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your modem 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 modem 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 modem router using the NAT-assigned source port (for example, port 33333) as the destination port and the IRC server also sends an “identify” message to your modem router with destination port 113.
6. When your modem 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 modem router restores the original address information replaced by NAT and sends this reply message to your computer.
7. When your modem 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 modem 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 modem router eventually senses a period of inactivity in the communications. The modem router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

13 Diagnostics and Troubleshooting

13

This chapter provides information to help you diagnose and solve problems that might occur with the modem router.

This chapter contains the following sections:

- *Perform Diagnostics*
- *Quick Tips for Troubleshooting*
- *Troubleshoot with the LEDs*
- *You Cannot Log In to the Modem Router*
- *View and Manage the Event Log*
- *Troubleshoot the Internet Connection*
- *Changes Are Not Saved*
- *Troubleshoot the WiFi Connectivity*
- *TCP/IP Network Not Responding*

Perform Diagnostics

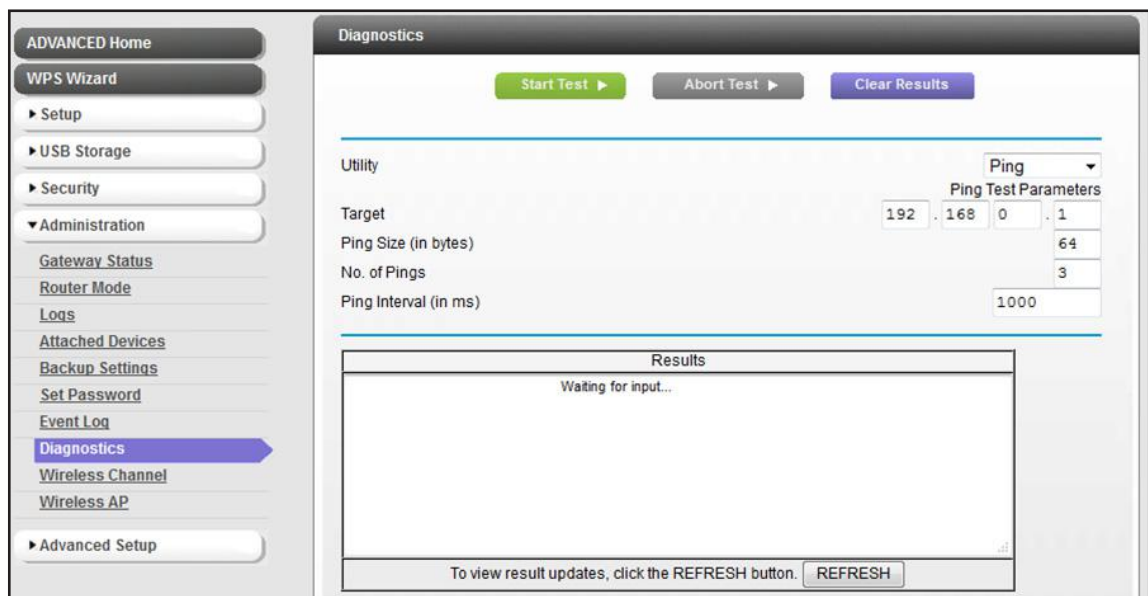
The modem router lets you perform various diagnostic tasks. For normal operation, these tasks are not required.

Ping an IP Address

Use this test to send a ping packet request to an IP address to test the connection. If the request times out because no reply is received, the destination might be unreachable. However, some network devices can be configured not to respond to a ping.

➤ **To ping an IP address:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Administration > Diagnostics**.



By default, **Ping** is selected from the **Utility** menu.

6. Enter the ping settings.

The following table describes the fields for the ping settings on the Diagnostics page.

Field	Description
Target	Enter the IP address of the device that you want to ping.
Ping Size (in bytes)	Enter the size of the ping packet. By default, the packet size is 64 bytes.
No. of Pings	Enter the number of times that the IP address is pinged. By default, the ping is sent three times.
Ping Interval (in ms)	Enter the interval between the consecutive pings. By default, the interval is 1000 ms.

- Click the **Start Test** button.

The Results field displays the results of the ping test.

- If the test does not complete, click the **Abort Test** button and try again.
- To refresh the results in the Results field, click the **REFRESH** button at the bottom of the field.
- To remove all information from the Results field, click the **Clear Results** button.

Trace a Route

Use this test to trace a route to an IP address or host name to test the connection. If you use a host name, you can also use this test to resolve the name to an IP address. If the request times out because no reply is received, the destination might be unreachable. However, some network devices can be configured not to respond to a traceroute request.

➤ To trace a route:

- Launch an Internet browser from a computer or WiFi device that is connected to the network.
- Type **http://www.routerlogin.net**.
A login window opens.
- Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
- Click the **OK** button.
The BASIC Home page displays.
- Select **ADVANCED > Administration > Diagnostics**.
The Diagnostics page displays.
- From the **Utility** menu, select **Traceroute**.

7. Enter the traceroute settings.

The following table describes the fields for the traceroute settings on the Diagnostics page.

Field	Description
Target (IP address or Name)	Enter the IP address or host name of the device that you want to trace.
Max Hops	Enter the maximum number of hops for the trace. By default, the maximum number of hops is 30.
Data Size (in bytes)	Enter the size of the probe packet. By default, the probe packet size is 32 bytes.
Base Port	Enter the port from which the probe packet is sent. By default, the port number is 33434.
Resolve Host	If you enter a host name, specify whether the name is resolved to an IP address by selecting one of the following options from the Resolve Host menu: <ul style="list-style-type: none"> • Off. The name is not resolved to an IP address. • On. The name is resolved to an IP address.

8. Click the **Start Test** button.

The Results field displays the results of the ping test.

Note: By default, after 30 hops, a traceroute times out.

9. To refresh the results in the Results field, click the **REFRESH** button at the bottom of the field.

10. To remove all information from the Results field, click the **Clear Results** button.

Quick Tips for Troubleshooting










The following table includes tips for troubleshooting some common problems.

Table 5. Quick tips for troubleshooting

Problem	Possible Solution
Your network is unresponsive or does not function normally.	Restart your network: <ol style="list-style-type: none"> 1. Turn off the modem router. 2. Turn on the modem router 3. Wait two minutes.
Your cannot connect over an Ethernet cable to the modem router.	<ul style="list-style-type: none"> • Make sure that the Ethernet cables are securely plugged in. • Make sure that your computer or device does not use a static IP address but is configured to receive an IP address automatically with DHCP. (For most devices, DHCP is the default setting.)
You cannot connect over WiFi to the modem router.	<ul style="list-style-type: none"> • Make sure that the WiFi settings in your WiFi device and modem router match exactly. For a device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the modem router and WiFi computer must match exactly. The default SSID and password are on the product label (see Product Label on page 23). • Make sure that your WiFi device supports the security that you are using for your WiFi network (WEP, WPA, or WPA2). For information about WiFi security settings, see Manage the Basic WiFi Settings and WiFi Security of the Main Network on page 36. • Make sure that the modem router is not too far from your WiFi device or too close: <ul style="list-style-type: none"> - Move your WiFi device near the modem router but at least 6 feet (1.8 meters) away and see if the signal strength improves. - Make sure that the WiFi signal is not blocked by objects between the modem router and your WiFi device. • Make sure that the WiFi LED for the 2.4 GHz radio or 5 GHz radio that you want to connect to is not off. If WiFi LED for a radio is off, the WiFi radio might be disabled. For more information about the WiFi radios, see Control the WiFi Radios on page 155. • Make sure that the modem router's SSID broadcast is not disabled. If the modem router's SSID broadcast is disabled, the WiFi network name is hidden and does not display in your WiFi device's scanning list. To connect to a hidden network, you must enter the network name and the WiFi password. For more information about the SSID broadcast, see Manage the Basic WiFi Settings and WiFi Security of the Main Network on page 36. • Make sure that your WiFi device does not use a static IP address but is configured to receive an IP address automatically with DHCP. (For most devices, DHCP is the default setting.)


Troubleshoot with the LEDs

When you turn on the power, the LEDs light as described here:

1. When power is first applied, the Power LED  lights red for a second and then turns green.
2. After about 15 seconds, the Downstream LED , Upstream LED , and Internet LED  start blinking green.
3. After about 35 seconds, the 2.4 GHz LED  lights green.
4. After about 45 seconds, the 5 GHz LED  lights green.
5. When the modem router establishes external connections, the following occurs:
 - After the modem router establishes a downstream connection, the Downstream LED  lights solid amber or solid green.
 - After the modem router establishes an upstream connection, the Upstream LED  lights solid amber or solid green.
 - After the modem router establishes an Internet connection, the Internet LED  lights solid green. At this point, the modem router is ready for use.

Note: Whether the Ethernet LED  lights depends on whether an Ethernet device is connected to the modem router.


Power LED Is Off

If the Power LED  and other LEDs are off when your modem router is turned on, do the following:

- Check that the power cord is correctly connected to your modem router and that the power supply adapter is correctly connected to a functioning power outlet.
- Check that you are using the 12 VDC 2.5A power adapter that NETGEAR supplied for this product.

If the error persists, a hardware problem might exist. For recovery instructions or help with a hardware problem, contact technical support at netgear.com/support.

Power LED Is Red

When the modem router is turned on, the Power LED  lights red for one second and then turns green. If the Power LED does not turn green, a fault exists within the modem router. In this situation, turn the power off and on to see if the modem router recovers. If the Power LED still does not turn green, do the following:

- Turn the power off and on one more time to see if the modem router recovers.
- Clear the modem router's configuration to factory defaults (see *Return the Modem Router to Its Factory Default Settings* on page 113). This sets the modem router's IP address to 192.168.0.1.


If the error persists, an unrecoverable firmware or hardware problem occurred. For recovery instructions or help with a hardware problem, contact technical support.


If the Power LED turns red in any other situation, the modem router became overheated and entered thermal cutoff mode. In this situation, do the following:

1. Turn the power off.
2. Let the modem router cool.
Move the modem router away from heat sources (such as a TV, DVD player, or speakers) and keep it vertical in open air.
3. After the modem router cooled, turn the power on.


WiFi LED Is Off

If a WiFi LED stays off, the associated WiFi radio in the modem router is off. For information about turning on the WiFi radio, see *Control the WiFi Radios* on page 155.

If you turn on the 2.4 GHz WiFi radio, the 2.4 GHz WiFi LED  lights green.

If you turn on the 5 GHz WiFi radio, the 5 GHz WiFi LED  lights green.

Ethernet LED Is Off

If the Ethernet LED  does not light when you connect a device, check the following:

- The Ethernet cable connections are secure at the modem router and at the device.
- The power is turned on to the connected device.
- You are using the correct cable.

You Cannot Log In to the Modem Router

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the modem router.
- If the computer is set to a static or fixed IP address (this setting is uncommon), either change the computer to obtain an IP address automatically from the modem router through DHCP, or change the IP address of the computer to a static or fixed IP address in the 192.168.0.2–192.168.0.254 range.
- Make sure that your computer can reach the modem router's DHCP server. Recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the modem router and reboot your computer.

- If your modem router's IP address was changed and you do not know the current IP address, use an IP scanner application to detect the IP address. If you still cannot find the IP address, clear the modem router's configuration to factory defaults. This sets the modem router's IP address to 192.168.0.1. For more information, see *Return the Modem Router to Its Factory Default Settings* on page 113 and *Factory Default Settings* on page 195.
- Make sure that Java, JavaScript, or ActiveX is enabled in your browser. If you are using Internet Explorer, click the **Refresh** button to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The user name is **admin**, and the default password is **password**. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your modem router behind an existing router in your network, turn on router mode to enable the modem router to function as a bridge to the router (see *Cable the Modem Router to a Router and Use Bridge Mode* on page 17).

View and Manage the Event Log

The event log is a detailed record of events that occur between the modem router and the cable service provider's cable modem termination system (CMTS). Such events include firmware downloads, DOCSIS time-outs, WiFi channel changes, and login authentications to the CMTS.

The event log might help your cable service provider to troubleshoot problems and isolate faults that might occur. Technical support might ask about events that are listed in the event log.

➤ To view or clear the event log:

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > Administration > Event Log**.



The Event Log page displays a table that shows, for each event, the time that the event occurred, the priority of the event (0 being the highest priority and 6 the lowest), and a detailed description.



The previous figure show an event with priority 3 that occurs when the modem router cannot synchronize its time with a server.

6. To refresh the page, click the **Refresh** button.
The information onscreen is updated.
7. To clear the log entries, click the **Clear Log** button.
All entries are removed from the table.

Troubleshoot the Internet Connection

If your modem router cannot access the Internet, check the cable connection.

Troubleshoot the Cable Link

If your modem router is unable to access the Internet, first determine whether the cable link with the service provider is working. The Downstream LED  and Upstream LED  indicate the state of this connection.

Downstream and Upstream LEDs Are Amber or Green

If the Downstream and Upstream LEDs light solid amber or solid green (or one LED lights solid green and the other lights solid amber), the cable connection is good. You can be confident that the service provider connected your line correctly and that your wiring is correct.

The Downstream LED or Upstream LED Is Blinking Green

If the Downstream LED is blinking green, the modem router is attempting to make a downstream cable connection (which allows you to receive information) with the service provider.

If the Upstream LED is blinking green, the modem router is attempting to make an upstream cable connection (which allows you to send information) with the service provider.


If the modem router establishes a cable connection, the Downstream and Upstream LEDs turn solid amber or solid green (or one LED lights solid green and the other lights solid amber). This connection process generally lasts several minutes.

Downstream and Upstream LEDs Are Off

If both the Downstream and Upstream LEDs are off, the modem router cannot get a connection with your cable Internet provider.


Make sure that you cabled the modem router correctly (see [Cable the Modem Router](#) on page 14). If the cabling is correct but the modem router cannot get a connection, contact your cable Internet provider.

Internet LED Is Off

If the Internet LED  is off, the modem router cannot connect to the Internet. Verify the following:

- Check that the IP address information for the ISP connection is correct (see [View or Manually Set Up the IPv4 Internet Settings](#) on page 30). In most cases, the ISP assigns IP addresses dynamically.
- Check to see if your ISP is experiencing a problem—it might not be that the modem router cannot connect to the Internet, but rather that your ISP cannot provide an Internet connection.

Obtain an Internet IP Address

If the modem router cannot access the Internet but the Internet LED  is green, see if the modem router can obtain an Internet IP address from the ISP. Unless the modem router is assigned a static IP address, the modem router requests an IP address from the ISP. You can determine whether the request was successful using the web management interface.

➤ **To check the Internet IP address:**

1. Launch an Internet browser from a computer or WiFi device that is connected to the network.
2. Type **http://www.routerlogin.net**.
A login window opens.
3. Type **admin** for the user name and type your password.
If you did not yet personalize your password, type **password** for the password.
4. Click the **OK** button.
The BASIC Home page displays.
5. Select **ADVANCED > ADVANCED Home**.
The ADVANCED Home page displays.
6. In the Internet Port pane, check that the IP Address field shows a valid IP address.
If the field shows 0.0.0.0, your modem router did not obtain an IP address from your ISP.

If your modem router cannot obtain an IP address from the ISP, check that the IP address information for the ISP connection is correct (see *View or Manually Set Up the IPv4 Internet Settings* on page 30). In most cases, the ISP assigns IP addresses dynamically.

Troubleshoot Internet Browsing

If your modem router can obtain an IP address but your computer is unable to load any web pages from the Internet, it might be for one of 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 (see *Unblock the Traffic Meter After the Traffic Limit Is Reached* on page 120). If your 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 when you set up the modem router, reboot your computer and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- The modem router might not be configured as the TCP/IP router on your computer.
For information about TCP/IP problems, see *TCP/IP Network Not Responding* on page 192.
If your computer obtains its information from the modem router by DHCP, reboot the computer and verify the modem router address.

Changes Are Not Saved

If the modem router does not save the changes that you make in the modem router web management 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. The changes occurred, but the old settings might be in the web browser's cache.

Troubleshoot the WiFi Connectivity


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


- Make sure that the WiFi settings in your WiFi device and modem router match exactly.

For a device that is connected over WiFi, the WiFi network name (SSID) and WiFi security settings of the modem router and WiFi computer must match exactly. The default SSID and password are on the product label (see [Product Label](#) on page 23).

- Does the WiFi device that you are using find your WiFi network?

If a WiFi LED stays off, the associated WiFi radio in the modem router is off. For information about turning on the WiFi radio, see [Control the WiFi Radios](#) on page 155.

If you turn on the 2.4 GHz WiFi radio, the 2.4 GHz WiFi LED  lights green.

If you turn on the 5 GHz WiFi radio, the 5 GHz WiFi LED  lights green.

- If you disabled the modem router's SSID broadcast, your WiFi network is hidden and does not display in your WiFi client's scanning list. (By default, SSID broadcast is enabled.) For more information, see [Manage the Basic WiFi Settings and WiFi Security of the Main Network](#) on page 36.
- Does your WiFi device support the security that you are using for your WiFi network (WEP, WPA, or WPA2)? For information about changing the WiFi security, see [Manage the Basic WiFi Settings and WiFi Security of the Main Network](#) on page 36.

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

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

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

TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers provide a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

Test the LAN Path to Your Modem Router

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

➤ **To ping the modem router from a Windows computer:**

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

```
ping 192.168.0.1
```

3. Click the **OK** button.

A message such as the following one displays:

```
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, the network might not be configured correctly. Do the following:

- Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
- Verify that the IP address for your modem router and your computer are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After you verify that the LAN path works correctly, test the path from your computer to a remote device:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type

```
ping -n 10 IP address
```

where *IP address* is the IP address of a remote device such as your cable service provider's DNS server.

If the path is functioning correctly, replies as described in [Test the LAN Path to Your Modem Router](#) on page 192 display. If you do not receive replies, do the following:

- Check to see that your computer uses the IP address of your modem router as the default modem router. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the modem router is listed as the default router.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- If the modem router cannot obtain an IP address from the cable service provider, the cable service provider might check for a host name, a domain name, or both. Assign the host name, domain name, or both. For more information, see [View or Manually Set Up the IPv4 Internet Settings](#) on page 30.

A Factory Default Settings and Specifications



This appendix includes the factory default settings and technical specifications for the modem router.

This appendix contains the following sections:

- *Factory Default Settings*
- *Technical and Environmental Specifications*

Factory Default Settings

You can return the modem router to its factory default settings (see [Return the Modem Router to Its Factory Default Settings](#) on page 113). The following table shows the factory default settings.

Table 6. Factory default settings

Feature		Default Settings
Router login	User login URL	http://www.routerlogin.net, http://www.routerlogin.com, or http://192.168.0.1
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Local area network (LAN)	LAN IP address	192.168.0.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.0.10 to 192.168.0.254
	DHCP start IP address	192.168.0.11
	DHCP end IP address	192.168.0.254
	Reserved IP address for ReadySHARE	192.168.0.10
	UPnP	Enabled
Wide area network (WAN) and security	Port scan and DoS protection	Disabled
	Default DMZ server	Disabled
	Respond to ping on Internet port	Disabled
	MTU size	Uses the maximum MTU value for best throughput
	SIP ALG	Enabled
	Remote management over WAN	Disabled
	Inbound communication from the Internet	Disabled, except for traffic on port 80 (the HTTP port) in response to requests from the LAN
	Outbound communication to the Internet	Enabled
	Network address translation	Enabled (nonconfigurable)
	Stateful packet inspection	Enabled (nonconfigurable)
	Sites blocked	None
	Services blocked	None

Table 6. Factory default settings (continued)

Feature		Default Settings
Main WiFi network	WiFi communication	Enabled (2.4 GHz and 5 GHz bands)
	SSID name	See product label
	SSID broadcast	Enabled (2.4 GHz and 5 GHz bands)
	Security	WPA2-PSK (AES)
	WiFi network key (passphrase)	See product label
	Country/region	United States, nonconfigurable
	RF channel	<ul style="list-style-type: none"> • 2.4 GHz band: Auto • 5 GHz band: 153
	Transmission speed	Auto ¹
	Operating mode	<ul style="list-style-type: none"> • 2.4 GHz band: Up to 300 Mbps • 5 GHz band: Up to 1.3 Gbps
Guest WiFi network	WiFi communication	Disabled
	SSID name	<ul style="list-style-type: none"> • 2.4 GHz band: NETGEAR-Guest • 5 GHz band: NETGEAR-5G-Guest
	SSID broadcast	Enabled (2.4 GHz and 5 GHz bands)
	Security	None (open network)
	Allow guests to access main network	Disabled (2.4 GHz and 5 GHz bands)
General and advanced WiFi settings	Radio transmission power	100%, nonconfigurable (2.4 GHz and 5 GHz bands)
	Fragmentation length	2346 (2.4 GHz and 5 GHz bands)
	CTS/RTS threshold	2347 (2.4 GHz and 5 GHz bands)
	Preamble mode	Long Preamble, nonconfigurable (2.4 GHz and 5 GHz bands)
	Beamforming transmission	Enabled (5 GHz band only)
	Beamforming reception	Enabled (5 GHz band only)
	WMM	Enabled (2.4 GHz and 5 GHz bands)
	PMF	Disabled (2.4 GHz and 5 GHz bands)
	WMF	Enabled (2.4 GHz and 5 GHz bands)
ATF	Disabled (2.4 GHz and 5 GHz bands)	

Table 6. Factory default settings (continued)

Feature		Default Settings
WPS	WPS capability	Enabled
	Modem router's PIN	Enabled; see the web management interface (path ADVANCED > Advanced Setup > Wireless Settings)
	Keep Existing Wireless Settings	Enabled (2.4 GHz and 5 GHz bands)

1. Maximum WiFi 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 and Environmental Specifications

Table 7. Modem router specifications

Feature	Description
Data and routing protocols	TCP/IP, DHCP server and client, DNS relay, NAT (many-to-one), TFTP client, VPN pass-through, DNS, UPnP
Power adapter	<ul style="list-style-type: none"> North America (input): 120V, 60 Hz, 1A input North America (output): 12 VDC @ 2.5A, 30W maximum output
Dimensions and weight	<ul style="list-style-type: none"> 7.68 by 7.79 by 2.52 in. (195 by 198 by 64 mm) 1.2 lb (0.54 kg)
WAN port	One coaxial cable connector DOCSIS 3.0. backward compatible with DOCSIS 2.0, 1.1, and 1.0
Ethernet ports	Two 10/100/1000BASE-T, RJ-45 autosensing ports
USB ports	One USB 2.0 ports
WiFi	<ul style="list-style-type: none"> 2.4 GHz band: Up to 300 Mbps or 802.11b/g/n devices 5 GHz band: Up to 1.3 Gbps for 802.11a/n/ac devices
WiFi channels	<ul style="list-style-type: none"> 2.4 GHz band: Auto or a single channel from 1 through 11 5 GHz band: 36, 40, 44, 48, 149, 153, 157, 161 or 165
Maximum computers per WiFi network	Limited by the amount of WiFi network traffic generated by each node
Operating frequency ranges	<ul style="list-style-type: none"> 2.4 GHz band: 2.412–2.462 GHz 5 GHz band: 5.18–5.24 + 5.745–5.825 GHz

Table 7. Modem router specifications (continued)

Feature	Description
802.11 authorization and encryption	<ul style="list-style-type: none"> • WPA2-PSK [AES] • WPA-PSK [TKIP] + WPA2-PSK [AES] • WPA/WPA2 Enterprise Legacy methods, available only in the Up to 54 Mbps mode: <ul style="list-style-type: none"> • WEP • WPA-PSK [TKIP]
Operating temperature	32° to 104°F (0° to 40°C)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	FCC part 15B/C/E
Safety standards	UL60950-1