

NETGEAR®

A750 Wireless Dual Band Gigabit Router JR6150

User Manual



November 2013
202-11270-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for purchasing this NETGEAR product.

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, additional documentation, and 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>.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved.

Compliance

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

Contents

Chapter 1 Hardware Setup

Unpack Your Router	8
Position Your Router	9
Hardware Features	10
Front Panel	10
Back Panel	12
Product Label	13

Chapter 2 Get Started with NETGEAR genie

Router Setup Preparation	15
Use Standard TCP/IP Properties for DHCP	15
Gather ISP Information	15
Wireless Devices and Security Settings	15
Types of Logins and Access	15
NETGEAR genie Setup	16
Use NETGEAR genie after Installation	17
Upgrade Router Firmware	18
Change the Password	18
Password Recovery	19
Add Wireless Devices or Computers to Your Network	21
Manual Method	21
Wi-Fi Protected Setup Method	21

Chapter 3 genie BASIC Settings

Internet Setup	24
Basic Wireless Settings	25
WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode	28
WPA/WPA2 Enterprise	29
WEP	30
Attached Devices	32
Parental Controls	33
Guest Networks	36
FastLane	38

Chapter 4 genie ADVANCED Home

Setup Wizard	40
WPS Wizard	41
WAN Setup	43

Default DMZ Server	44
Change the MTU Size	45
LAN Setup	47
Use the Router as a DHCP Server	49
Address Reservation	50
Quality of Service Setup	52
Wi-Fi Multimedia Quality of Service for Wireless Traffic	52
Quality of Service Priority Rules and Internet Access	52
Bandwidth Control	53
Manage QoS Rules	54

Chapter 5 USB Port

Enhance Your Local Network	65
Set Up Network Storage	66
Connect or Safely Remove a USB Drive	66
View or Configure a USB Drive	67
Configure the USB Storage Device and Access Settings	68
Configure the Available Network Folders	70
Specify Approved USB Devices	74
Access and Share Your Network Storage	75
Common Uses of Network Sharing	75
Access Your USB Storage Device Locally	77
Access Your USB Storage Device Remotely	78
Set Up a Network Printer	79

Chapter 6 Security

Keyword Blocking of HTTP Traffic	85
Port Filtering to Block Services	87
Schedule Blocking	88
Security Event Email Notifications	89

Chapter 7 Administration

View Router Status	92
Router Information Pane	92
Internet Port Pane	93
Statistics	94
Connection Status	96
Wireless Settings Panes	98
Guest Network Panes	99
View Logs of Web Access or Attempted Web Access	100
Manage the Configuration File	101
Back Up Settings	101
Restore Configuration Settings	102
Erase	103
Upgrade the Router Firmware	104

Chapter 8 Advanced Settings

Advanced Wireless Settings	107
Control the Wireless Radio	107
Set Up a Wireless Schedule	108
View or Change WPS Settings	109
Set Up a Wireless Access List by MAC Address	110
Wireless AP	112
Wireless Repeating Function	114
Set Up the Base Station	115
Set Up a Repeater	116
Port Forwarding and Port Triggering Configuration Concepts	118
Remote Computer Access Basics	118
Port Triggering to Open Incoming Ports	120
Port Forwarding to Permit External Host Communications	121
How Port Forwarding Differs from Port Triggering	122
Set Up Port Forwarding to Local Servers	122
Add a Custom Service	123
Edit or Delete a Port Forwarding Entry	125
Application Example: Make a Local Web Server Public	126
Set Up Port Triggering	127
Dynamic DNS	131
Static Routes	132
Remote Management	136
Universal Plug and Play	138
Traffic Meter	139

Chapter 9 Troubleshooting

Quick Tips	144
Sequence to Restart Your Network	144
Check Ethernet Cable Connections	144
Wireless Settings	144
Network Settings	144
Troubleshooting with the LEDs	145
Power/Check LED Is Off or Blinking	145
Power/Check LED Stays Amber	145
LEDs Never Turn Off	146
Internet or Ethernet LAN Port LEDs Are Off	146
Wireless LEDs Are Off	146
WPS/FastLane Button Blinks Amber	146
Cannot Log In to the Router	147
Cannot Access the Internet	147
Troubleshooting PPPoE	149
Troubleshooting Internet Browsing	149
Changes Not Saved	150
Wireless Connectivity	150
Restore the Factory Settings and Password	151
Troubleshoot Your Network Using the Ping Utility	151

Test the LAN Path to Your Router 151

Test the Path from Your Computer to a Remote Device 152

Appendix A Supplemental Information

Factory Default Settings 154

Specifications 155

Index

Hardware Setup

1

Get to know your router

The A750 Wireless Dual Band Gigabit Router JR6150 provides an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). It is compatible with all major DSL Internet service providers, lets you block unsafe Internet content and applications, and protects the devices (computers, gaming consoles, and so on) that you connect to your home network.

If you have not already set up your new router using the installation guide that comes in the box, *Chapter 2, Get Started with NETGEAR genie* walks you through the hardware setup. *Chapter 3, genie BASIC Settings*, explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your Router*
- *Position Your Router*
- *Hardware Features*

For information about ReadySHARE features in your product, see *Chapter 5, USB Port*, and visit www.netgear.com/readymshare.

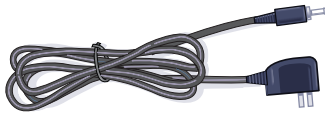
For more information about the topics covered in this manual, visit the support website at <http://support.netgear.com>.

Unpack Your Router

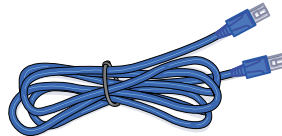
Open the box and remove the router, power adapter, cable, and installation guide.



JR6150 router



Power adapter



Ethernet cable

Figure 1. Check the package contents

Your box contains the following items:

- A750 Wireless Dual Band Gigabit Router JR6150
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Installation guide with cabling and router setup instructions

If any parts are incorrect, missing, or damaged, contact your NETGEAR dealer.

Position Your Router

The router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your router. For example, the thickness and number of walls the wireless signal passes through can limit the range.

➤ **To position your router:**

1. Place your router near the center of the area where your computers and other devices operate, and within line of sight to your wireless devices.
2. Make sure that the router is within reach of an AC power outlet and near Ethernet cables for wired computers.
3. Place the router in an elevated location, minimizing the number walls and ceilings between the router and your other devices.
4. Place the router away from electrical devices such as these:
 - Ceiling fans
 - Home security systems
 - Microwaves
 - Computers
 - Base of a cordless phone
 - 2.4 GHz cordless phone
5. Place the router away from large metal surfaces, large glass surfaces, insulated walls, and other surfaces such as these:
 - Solid metal door
 - Aluminum studs
 - Fish tanks
 - Mirrors
 - Brick
 - Concrete

Hardware Features

Before you cable your router, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

Front Panel

The router front panel has the status LEDs and icons shown in the following figure.

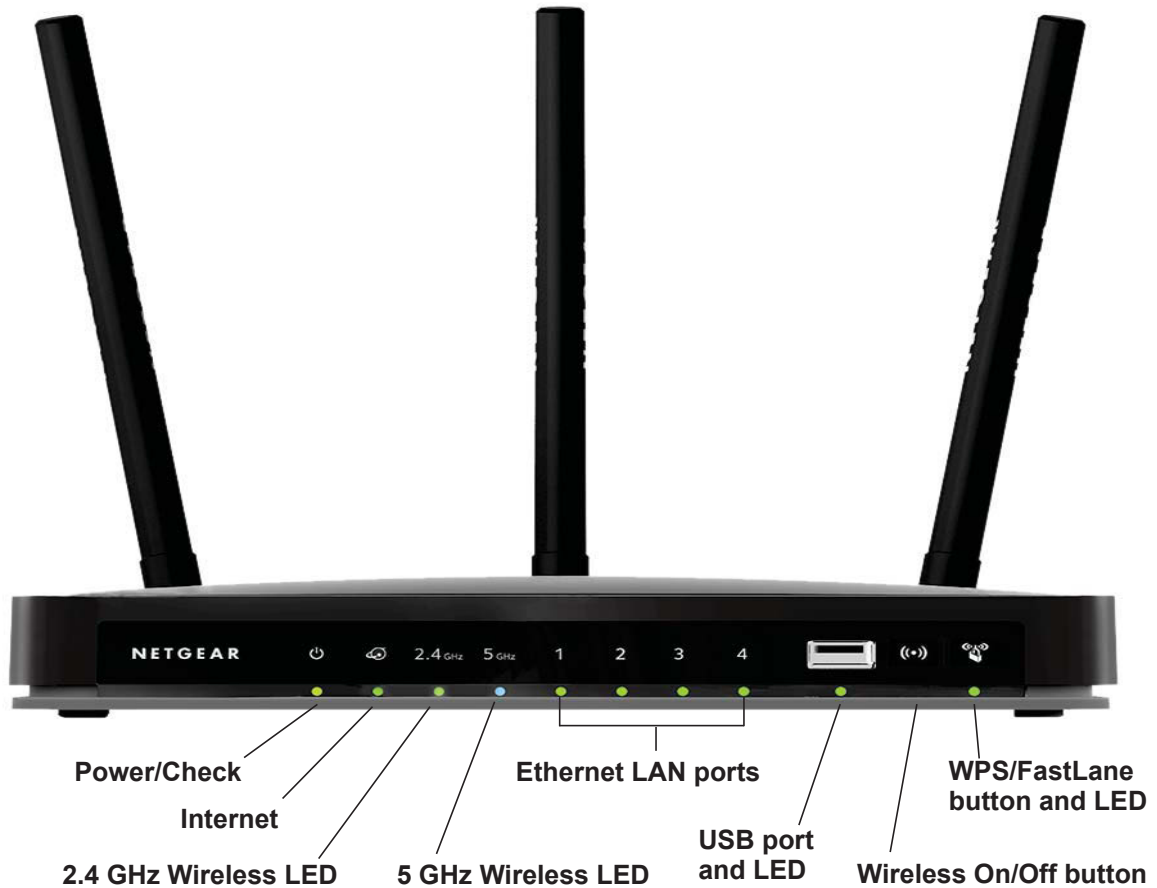


Figure 2. Router, front view

Table 1. Front panel LED descriptions

LED	Description
Power/Check 	Solid green. The startup is completed, and the router is ready. Blinking green. The firmware is corrupted (visit http://www.netgear.com/support). Blinking amber. The firmware is upgrading, or the Restore Factory Settings button was pressed. Off. Power is not supplied to the router.
Internet 	Solid green. An IP address was received; the router is ready to transmit data. Solid amber. The router detected the Ethernet cable connection. Off. No Ethernet cable is connected to the router.
2.4 GHz Wireless 	Solid green. The wireless interface is enabled. Blinking green. The wireless network is communicating data. Off. The wireless interface is turned off.
5 GHz Wireless 	Solid blue. The wireless interface is enabled. Blinking green. The wireless network is communicating data. Off. The wireless interface is turned off.
LAN ports 1–4 	Solid green. The local port is connected to a 1000 Mbps device. Blinking green. Data is being transmitted at 1000 Mbps. Solid amber. The local port is connected to a 10/100 Mbps device. Blinking amber. Data is being transmitted at 10/100 Mbps. Off. No link is detected on this port.
USB 	Solid green. The USB device is accepted by the router and is ready to be used. Blinking green. A USB device is in use. Off. No USB device is connected, or the Safely Remove Hardware button was clicked and it is now safe to remove the attached USB device.
WPS/FastLane 	Solid green. A WPS-capable or FastLane-capable device is accepted by the router and is ready to be used. Blinking green. The WPS-capable or FastLane-capable device can be associated with the router within two minutes. Off. No WPS or FastLane connection exists.

The WLAN and WPS buttons toggle the WLAN and WPS functions on and off, as follows:

-  **Wireless On/Off button.** Pressing and holding the wireless LAN button for two seconds turns the 2.4 GHz and 5 GHz wireless radios on and off. If the Wireless LEDs are lit, the wireless radios are on. If the LEDs are off, the wireless radios are turned off and you cannot connect wirelessly to the router.

-  **WPS/FastLane button.** You can use this button to use WPS or FastLane to add a wireless device or computer to your wireless network. The LED below the **WPS/FastLane** button blinks green when the router is trying to add the wireless device or computer. The LED stays solid green when wireless security is enabled in the router.

Back Panel

The back panel has the buttons and connections shown in the following figure.

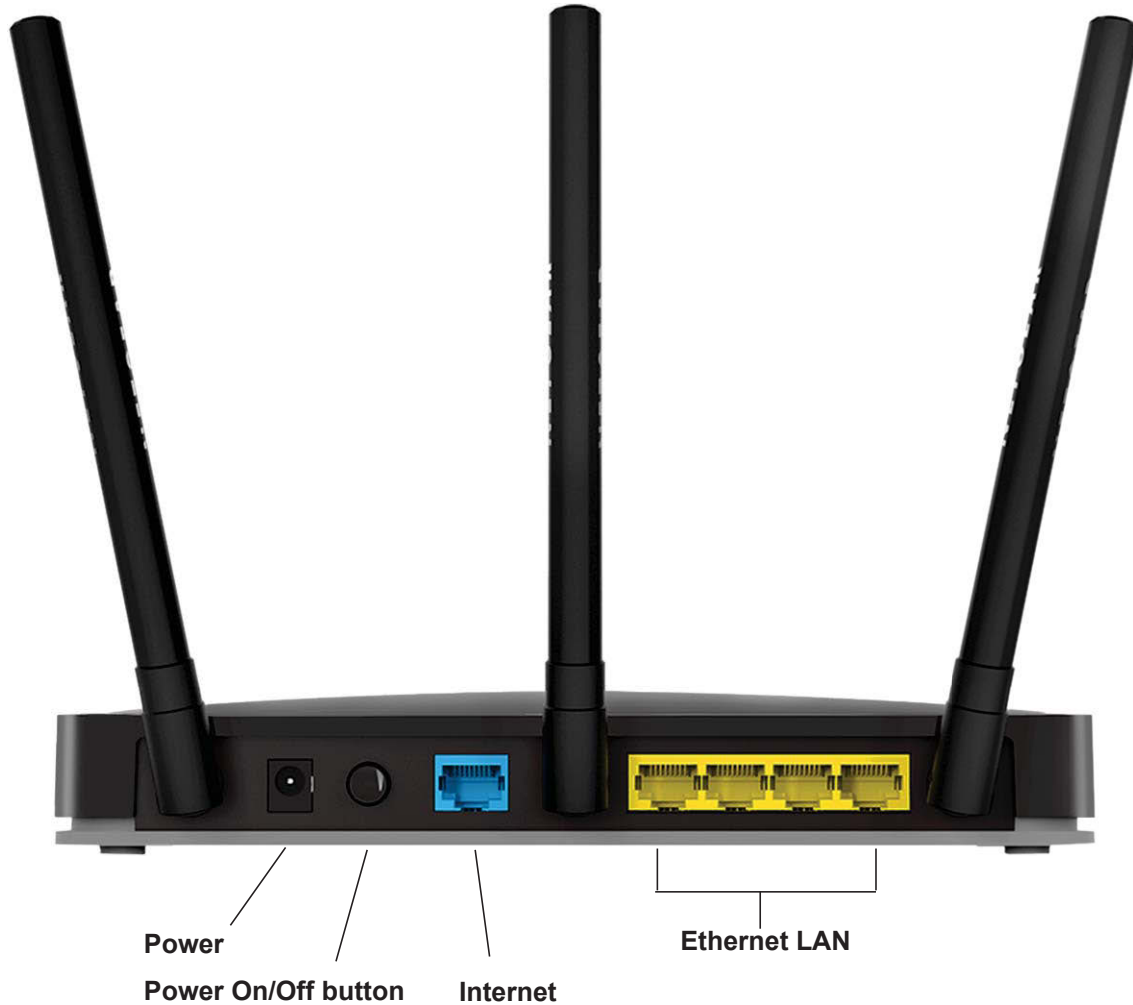


Figure 3. Router, rear view

Product Label

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

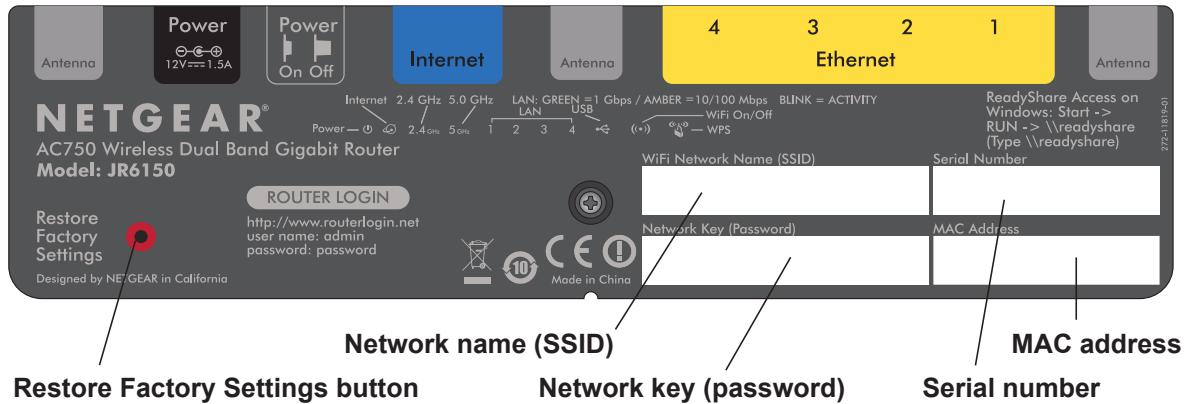


Figure 4. The label shows unique information about your router

See [Factory Default Settings](#) on page 154 for information about restoring factory settings.

2. Get Started with NETGEAR genie

2

Connect to the router

This chapter explains how to use NETGEAR genie to set up your router after you complete cabling as described in the installation guide.

This chapter contains the following sections:

- *Router Setup Preparation*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie after Installation*
- *Upgrade Router Firmware*
- *Change the Password*
- *Password Recovery*
- *Add Wireless Devices or Computers to Your Network*

Router Setup Preparation

You can set up your router with the NETGEAR genie automatically, or you can use the genie menus and screens to set up your router manually. However, before you start the setup process, you need to have your ISP information on hand and make sure the laptops, computers, and other devices in the network have the settings described in this section.

Use Standard TCP/IP Properties for DHCP

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

Gather ISP Information

For DSL broadband service, when your Internet service starts, your Internet service provider (ISP) typically gives you all of the information needed to connect to the Internet. You might need this information to set up the router to use your Internet service. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP login program on your computer to access the Internet. When you start an Internet application, your router automatically logs you in. You might need the following information to set up your router:

- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address settings (special deployment by ISP)

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the router. For information about the router's preconfigured security settings, see [Basic Wireless Settings](#) on page 25.

Types of Logins and Access

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

Types of logins:

- **Router login.** The login that your ISP provided logs you in to the router interface from NETGEAR genie. See [Use NETGEAR genie after Installation](#) on page 17 for details about this login.
- **ISP login.** This logs you in to your Internet service. Your service provider gave you this login information in a letter or some other way. If you cannot find this login information, contact your service provider.

- **Wireless network key or password.** Your router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the product label.

NETGEAR genie Setup

NETGEAR genie runs on any computer or device with a web browser. It is the easiest way to set up the router because it automates many of the steps and verifies that those steps have been successfully completed. It takes about 15 minutes to complete.

➤ To use NETGEAR genie to set up your router:

1. Turn the router on by pressing the **On/Off** button, if not done yet.
2. Make sure that your device is connected with an Ethernet cable (wired) or wirelessly (with the preset security settings listed on the product label) to your router.
3. Launch your Internet browser in one of the following ways:
 - The first time you set up the Internet connection for your router, the browser automatically goes to **http://www.routerlogin.net**, and the NETGEAR genie screen displays.
 - If you already used the NETGEAR genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR genie screen. See *Use NETGEAR genie after Installation* on page 17.

4. Follow the onscreen instructions to complete NETGEAR genie setup.

NETGEAR genie guides you through connecting the router to the Internet.

5. If the browser cannot display the web page, do the following:
 - Make sure that the computer is connected to the LAN Ethernet port or wirelessly to the router.
 - Make sure that the router is running. If it is, its Wireless LEDs are lit.
 - Close and reopen the browser to make sure that the browser does not cache the previous page.
 - Browse to **http://routerlogin.net**.
 - If the computer is set to a static or fixed IP address (this situation is uncommon), change it to obtain an IP address automatically from the router.
6. If the router does not connect to the Internet, do the following:
 - a. To be sure that you have selected the correct options and typed everything correctly, review the router's settings.
 - b. Contact your ISP to verify that you have the correct configuration information for your main Internet connection.
 - c. Read *Chapter 9, Troubleshooting*.

Use NETGEAR genie after Installation

When you first set up your router, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the router. You can use NETGEAR genie again if you want to view or change settings for the router.

1. Launch your browser from a computer or wireless device that is connected to the router.
2. Enter **http://www.routerlogin.net** or **http://www.routerlogin.com** in the web browser address bar.

A login screen displays.

A screenshot of the NETGEAR router login screen. It features a light beige background with a dark border. At the top left, the text "User name:" is followed by a dropdown menu showing "admin" with a small blue arrow icon to its right. Below this, the text "Password:" is followed by a text input field containing seven asterisks "*****". Under the password field is a checkbox labeled "Remember my password". At the bottom right, there are two buttons: "OK" and "Cancel".

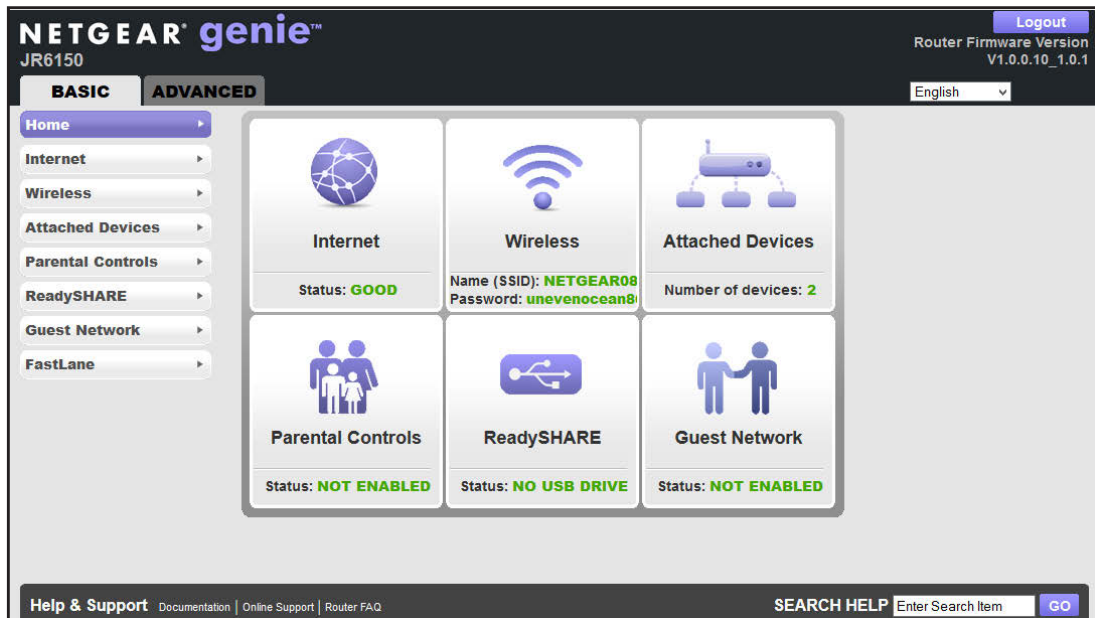
3. Enter the router user name and password.

The user name is **admin**. The default password is **password**. Both user name and password are case-sensitive.

Note: *The router user name and password are different from the user name and password for logging in to your Internet connection. For more information, see [Types of Logins and Access](#) on page 15.*

4. Click the **OK** button.

5. The BASIC Home screen displays.



Upgrade Router Firmware

When you set up your router and are connected to the Internet, the router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen. For more information about upgrading firmware, see [Upgrade the Router Firmware](#) on page 104.

Click the message when it displays, and click the **Yes button** to upgrade the router with the latest firmware. After the upgrade, the router restarts.



CAUTION:

Do not try to go online, turn off the router, shut down the computer, or do anything else to the router until the router finishes restarting and the Power/Check LED has stopped blinking for several seconds.

Change the Password

The default password that you use to log in to the router is password. NETGEAR recommends that you change this default password to a secure password.

Changing the default password is not the same as changing the password for wireless access. The label on your router shows your unique wireless network name (SSID) and the password (also referred to as the wireless network password or network key) for wireless access. For more information, see [Product Label](#) on page 13.

➤ **To change the default password that you use to log in to the router:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Administration > Set Password**.

3. Type the old password and type the new password twice in the fields on this screen.
4. If you want to be able to recover the password, select the **Enable Password Recovery** check box.

For more information, see *Password Recovery* on page 19.

5. Click the **Apply** button.

Password Recovery

NETGEAR recommends that you enable password recovery if you change the password for the router's user name of admin. Then you have an easy way to recover the password when it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➤ **To set up password recovery:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Administration > Set Password**.

3. Select the **Enable Password Recovery** check box.
4. Select two security questions and provide answers to them.
5. Click the **Apply** button.

➤ **To recover your password:**

1. In the address field of your browser, type **www.routerlogin.net**.
The login screen displays.
2. Click the **Cancel** button.
If password recovery is enabled, you are prompted to enter the serial number of the router. The serial number is on the product label.
3. Enter the serial number of the router.
4. Click the **Continue** button.
A screen displays requesting the answers to your security questions.
5. Enter the saved answers to your security questions.
6. Click the **Continue** button.
A screen displays your recovered password.
7. Click the **Login again** button.
The login screen displays.
8. With your recovered password, log in to the router.

Add Wireless Devices or Computers to Your Network

Choose either the manual or the WPS method to add wireless devices and other equipment to your wireless network.

You can set up a guest network to allow visitors at your home to use the Internet without giving them your wireless security key. For more information, see [Guest Networks](#) on page 36.

Manual Method

Use this method to connect your wireless devices to your home wireless network and your guests' wireless devices to your guest wireless network.

➤ **To connect WiFi devices manually to your router:**

1. From your wireless device, view the available wireless networks.
For more information, see the manual that came with your device.
2. From the list of available wireless networks, select the wireless network name (SSID) of the router.
The SSID is printed on the product label.
3. From your wireless device, initiate a wireless connection.
For more information, see the manual that came with your device.
4. When prompted by your wireless device, enter the wireless network key (password) of the router.
The password is printed on the product label.
5. From the screen of your wireless device, click the appropriate button to continue the connection procedure.
You are connected wirelessly to the router.
6. Repeat [Step 1](#) through [Step 5](#) for each wireless device that you want to connect to the router.

Wi-Fi Protected Setup Method

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

You can change the function of the **WPS/FastLane** button from WPS to FastLane. For more information, see [FastLane](#) on page 38.

➤ **To use WPS to join the wireless network:**

1. Press the **WPS/FastLane** button on the router's front panel.
2. Within two minutes, press the **WPS** button on your wireless device or follow the WPS instructions that came with the device.

The device is now connected to your router.

3. Repeat *Step 1* through *Step 2* to add other WPS wireless devices.

You can also use the WPS Wizard to add computers and other devices to your wireless network. For more information, see *WPS Wizard* on page 41.

3. genie BASIC Settings

3

Your Internet connection and network

This chapter explains the basic features of the router.

The chapter contains the following sections:

- *Internet Setup*
- *Basic Wireless Settings*
- *Attached Devices*
- *Parental Controls*
- *Guest Networks*
- *FastLane*

ReadySHARE allows you to enhance your local network with the router's USB port. For more information, see *Chapter 5, USB Port*.

Internet Setup

You can view or change ISP information.

➤ **To set up your Internet connection:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > Internet**.

The screenshot shows the 'Internet Setup' page in the 'BASIC' tab. The left sidebar has a menu with 'Internet' selected. The main area has a 'Test' button, a 'Cancel' button, and an 'Apply' button. The first section is 'Does your Internet connection require a login?' with radio buttons for 'Yes' and 'No'. Below this are fields for 'Account Name (If Required)' (containing 'JR6150') and 'Domain Name (If Required)'. The next section is 'Internet IP Address' with radio buttons for 'Get Dynamically from ISP' (selected) and 'Use Static IP Address'. Below this are fields for 'IP Address' (192.168.0.10), 'IP Subnet Mask' (255.255.255.0), and 'Gateway IP Address' (192.168.0.1). The final section is 'Domain Name Server (DNS) Address' with radio buttons for 'Get Automatically from ISP' (selected) and 'Use These DNS Servers'. Below this are fields for 'Primary DNS' (192.168.0.1) and 'Secondary DNS'.

3. Select one of the following radio buttons:
 - **Yes.** Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
 - **No.** Enter the account and domain names, only if needed.

These fields display when no login is required:

- **Account Name (If required).** Enter the account name provided by your ISP. This might also be called the host name.
- **Domain Name (If required).** Enter the domain name provided by your ISP.

These fields display when your ISP requires a login:

- **Internet Service Provider.** Select **PPPoE**, **L2TP**, or **PPTP**.
- **Login.** The login name provided by your ISP. This login name is often an email address.
- **Password.** The password that you use to log in to your ISP.
- **Service Name (if Required).** If your ISP provided a service name, enter it here.
- **Connection Mode.** Select **Always On**, **Dial on Demand**, or **Manually Connect**.
- **Idle Timeout (In minutes).** If you want to change the login time-out, enter a new value in minutes. This setting determines how long the router keeps the Internet

connection active when there is no Internet activity from the LAN. A value of 0 (zero) means never log out.

4. Enter the settings for the IP address and DNS server.

The default settings usually work fine. If you have problems with your connection, check the ISP settings. To change the default settings, do the following:

- **Internet IP Address:** Select one of the following radio buttons:
 - **Get Dynamically from ISP.** Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
 - **Use Static IP Address.** Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's router to which your router connects.
- **Domain Name Server (DNS) Address.** The DNS server is used to look up site addresses based on their names. Select one of the following radio buttons:
 - **Get Automatically from ISP.** Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
 - **Use These DNS Servers.** If you know that your ISP requires specific servers, select this radio button. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
- **Router MAC Address.** The Ethernet MAC address that the router uses on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your router to use your computer's MAC address (also called cloning). Select one of the following radio buttons:
 - **Use Default Address.** Use the default MAC address.
 - **Use Computer MAC Address.** The router captures and uses the MAC address of the computer that you are now using. You have to use the one computer that the ISP allows.
 - **Use This MAC Address.** Enter the MAC address that you want to use.

5. Click the **Apply** button.

Your settings are saved.

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

If the NETGEAR website does not display within one minute, see [Chapter 9, Troubleshooting](#).

Basic Wireless Settings

You can view or configure the wireless network setup.

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

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

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

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

➤ **To view or change basic wireless settings:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > Wireless**.

The screenshot displays the 'Wireless Network' configuration page in the router's web interface. The 'BASIC' tab is selected, and the 'Wireless' menu item is highlighted in the left sidebar. The page is divided into two main sections: 'Wireless Network (2.4GHz b/g/n)' and 'Wireless Network (5GHz a/n)'. The 2.4GHz section is active, showing a 'Select Region' dropdown set to 'Europe', an 'Name (SSID)' field with 'NETGEAR08', a 'Channel' dropdown set to 'Auto', and a 'Mode' dropdown set to 'Up to 300 Mbps'. Under 'Security Options', 'WPA2-PSK [AES]' is selected. A 'Passphrase' field contains 'unevenocan061'. The 5GHz section below shows a default 'Name (SSID)' of 'NETGEAR08-5G', 'Channel' set to 'Auto', 'Mode' set to 'Up to 450 Mbps', and 'WPA2-PSK' as the security option.

The 2.4 GHz and 5 GHz WiFi bands are configured separately.

3. To specify the location where the router is used, select from the countries in the **Region** list.
In Europe, the region is fixed to Europe and is not changeable.
4. Enter the SSID in the **Name (SSID)** field.

The SSID is also known as the wireless network name. The default SSID is randomly generated. **NETGEAR recommends that you do not change the default SSID.** If you do decide to change the name, enter a 32-character (maximum) name in this field. This field is case-sensitive.

5. Select the channel from the **Channel** list.

This setting is the wireless channel used by the gateway. For the 2.4 GHz band, select either **Auto** or a value from **1** through **13**. For products in the North America market, only Channels 1 through 11 can be operated. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best. The default setting is **Auto**, which means that the router selects a channel automatically.

Note: *When you use multiple access points, it is better if adjacent access points use different channels to reduce interference. In the 2.4 GHz band, the recommended channel spacing between adjacent access points is five channels (for example, use Channels 1 and 6, or 6 and 11).*

6. Select the mode from the **Mode** list.

Up to 300 Mbps is the default setting. **Up to 54 Mbps** supports 802.11g and 11b wireless devices. The **Up to 145 Mbps** setting allows 802.11n devices to connect at this speed.

7. To enable SSID broadcast, select the **Enable SSID Broadcast** check box.

This feature allows the router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default, but you can clear it to disable broadcast of the SSID.

8. To enable wireless isolation, select the **Enable Wireless Isolation** check box.

This feature allows wireless clients (computers or wireless devices) that join the network to use the Internet, but they cannot access each other or access Ethernet devices on the network.

9. Specify the security option.

You can change the wireless authentication and encryption option and the password (also referred to as the wireless network password or network key). The security that you select encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network.



WARNING:

NETGEAR recommends that you do not change the wireless security option or the password. Do not disable wireless security!

Set up the security options as discussed in the following sections:

- For information about how to set up WPA-PSK, WPA2-PSK, or WPA-PSK + WPA2-PSK mixed mode security, see [WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode](#) on page 28.
- For information about how to set up WPA/WPA2 enterprise security, see [WPA/WPA2 Enterprise](#) on page 29.
- For information about how to set up WEP security, see [WEP](#) on page 30.

Note: The **WEP** option displays only if you select **Up to 54 Mbps** from the **Mode** list.

10. Click the **Apply** button.

11. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:

- Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
- Does your wireless device or computer display on the Attached Devices screen? If it does, then it is connected to the network.
- If you are not sure what the SSID or password is, look on the label on your router.

WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode

These types of wireless security options use a pre-shared key (PSK), which is the same as a password, wireless network password, or network key.

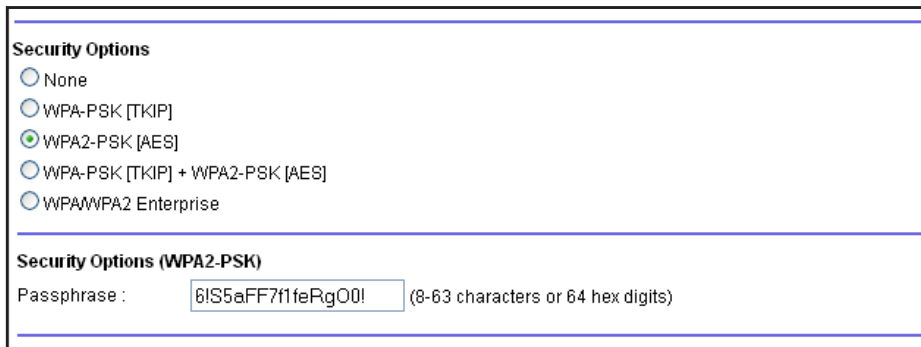
You can select from the following wireless PSK security options:

- **WPA-PSK [TKIP]**. Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption. This option supports speeds of up to 54 Mbps only.
- **WPA2-PSK [AES]**. Wi-Fi Protected Access version 2 (WPA2) data encryption provides strong data security with Advanced Encryption Standard (AES) encryption. This setting is the preset wireless security that is enabled by default. WPA2 provides the most reliable security. This option supports speeds of up to 300 Mbps. If not all clients in your network support WPA2, select WPA-PSK + WPA2-PSK mixed mode.
- **WPA-PSK [TKIP] + WPA2-PSK [AES]**. WPA-PSK + WPA2-PSK is referred to as mixed mode, which supports a combination of TKIP and AES encryption for both WPA and WPA2 clients. For WPA clients, this option supports speeds of up to 54 Mbps only. For WPA2 clients, this option supports speeds of up to 300 Mbps.
- **WPA/WPA2 Enterprise**. This security option is not for home use but is typically used in a business or enterprise. For more information, see [WPA/WPA2 Enterprise](#) on page 29.

Note: Some of these security options display only if you select **Up to 54 Mbps** from the **Mode** list.

➤ **To change the WPA wireless security option and password:**

1. Log in to the router.
For more information, see *Use NETGEAR genie after Installation* on page 17.
2. Select **BASIC > Wireless Settings**.
3. In the Security Options section, select one of the WPA options with PSK.



Security Options

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

Security Options (WPA2-PSK)

Passphrase : (8-63 characters or 64 hex digits)

4. In the associated **Passphrase** field, enter the password that you want to use.
The password is a text string from 8 to 63 ASCII characters or exactly 64 hexadecimal digits. A hexadecimal digit is one of the following characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A–F, or a–f.
Wireless clients must use the password to access the wireless network through the router.
5. Click the **Apply** button.

WPA/WPA2 Enterprise

This security option is not for home use but is typically used in a business or enterprise. WPA/WPA2 Enterprise does not use a password but supports 802.1x authentication, which requires an internal or external RADIUS server. A Remote Authentication Dial In User Service (RADIUS) server provides Authentication, Authorization, and Accounting (AAA) management to grant (or deny) computers access to your wireless network.

WPA/WPA2 Enterprise can support WPA [TKIP] for WPA clients only, WPA2 [AES] for WPA2 clients only, and WPA [TKIP] + WPA2 [AES]. WPA [TKIP] + WPA2 [AES] is a combination of TKIP and AES encryption for both WPA and WPA2 clients. WPA clients are supported at speeds of up to 54 Mbps only. WPA2 clients are supported at speeds of up to 300 Mbps.

WPA/WPA2 Enterprise supports five Extensible Authentication Protocol (EAP) authentication methods: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, and EAP-SIM.

➤ **To configure WPA/WPA2 Enterprise security:**

1. Log in to the router.
For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > Wireless Settings**.
3. In the Security Options section, select the **WPA/WPA2 Enterprise** radio button.

Security Options

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

Security Options (WPA/WPA2 Enterprise)

WPA Mode: WPA [TKIP] + WPA2 [AES] ▼

RADIUS server IP Address:

RADIUS server Port:

RADIUS server Shared Secret:

4. Select the WPA mode (**WPA [TKIP]**, **WPA2 [AES]**, or **WPA [TKIP] + WPA2 [AES]**).
5. Type the IP address of the RADIUS server.
The address can be on your LAN or it can be an external address.
6. Enter the port number for the RADIUS server in the range from 1 to 65535.
The default number is 1812.
7. Type the shared secret, which must be from 1 through 128 characters (the default value is blank).
The shared secret is case-sensitive.
8. Click the **Apply** button.

WEP

Wired Equivalent Privacy (WEP) security is an authentication and data encryption mode that is superseded by WPA-PSK and WPA2-PSK. WEP supports speeds of up to 54 Mbps and does not function with WPS.

Note: The **WEP** option displays only if you select **Up to 54 Mbps** from the **Mode** list.

➤ To configure WEP security:

1. Log in to the router.
For more information, see *Use NETGEAR genie after Installation* on page 17.
2. Select **BASIC > Wireless Settings**.

3. In the Security Options section, select the **WEP** radio button.

Security Options

☐ None
☒ WEP
☐ WPA-PSK [TKIP]
☐ WPA2-PSK [AES]
☐ WPA-PSK [TKIP] + WPA2-PSK [AES]
☐ WPAWPA2 Enterprise

Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: 64-bit

Security Encryption (WEP) Key

Passphrase: Generate

Key 1 ☒
 Key 2 ☐
 Key 3 ☐
 Key 4 ☐

4. In the **Authentication Type** list, select one of the following types:
- **Automatic.** If you enter a password in the **Passphrase** field and click the **Generate** button, the four keys are automatically generated.
 - **Shared Key.** If you select this option, you must select one key and enter the value manually.
5. In the **Encryption Strength** list, select the encryption key size:
- **64-bit.** Standard WEP encryption, using 40/64-bit encryption.
 - **128-bit.** Standard WEP encryption, using 104/128-bit encryption. This selection provides higher encryption security.
6. Depending on the authentication type, generate the key automatically or enter it manually:
- If the authentication type is **Automatic**, do the following
 - a. In the **Passphrase** field, enter a password.
 - b. Click the **Generate** button.

For 64-bit WEP, four different WEP keys are generated. For 128-bit WEP, only one WEP key is generated, and the four key fields are populated with the same WEP key.
 - If the authentication type is **Shared Key**, do the following
 - a. Specify the active key by selecting the **Key 1**, **Key 2**, **Key 3**, or **Key 4** radio button.
 - b. Enter the value for the key manually:
 - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, A–F). The key values are not case-sensitive.
 - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, A–F). The key values are not case-sensitive.
7. Click the **Apply** button.

Attached Devices

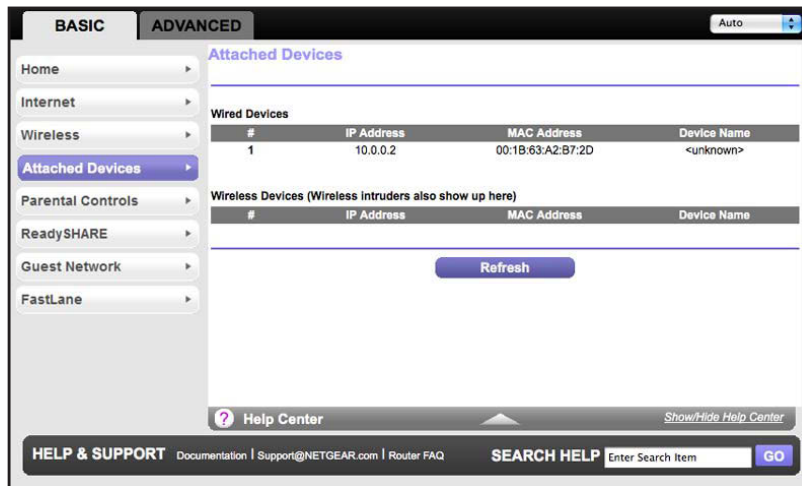
You can view all computers or devices that are currently connected to your network.

➤ **To view the attached devices:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > Attached Devices**.



Wired devices are connected to the router with Ethernet cables. Wireless devices have joined the wireless network. The following information displays:

- **# (number)**. The order in which the device joined the network.
 - **IP Address**. The IP address that the router assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.
 - **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.
 - **Device Name**. If the device name is known, it is shown here.
3. To update this screen, click the **Refresh** button.
 4. To secure your router against WiFi intruders, restrict wireless access.

For more information, see *Set Up a Wireless Access List by MAC Address* on page 110.

Parental Controls

The first time that you select **Parental Controls** from the BASIC Home screen, you are automatically directed to the NETGEAR website, where you can learn more about Live Parental Controls or download the application. The following screen displays:

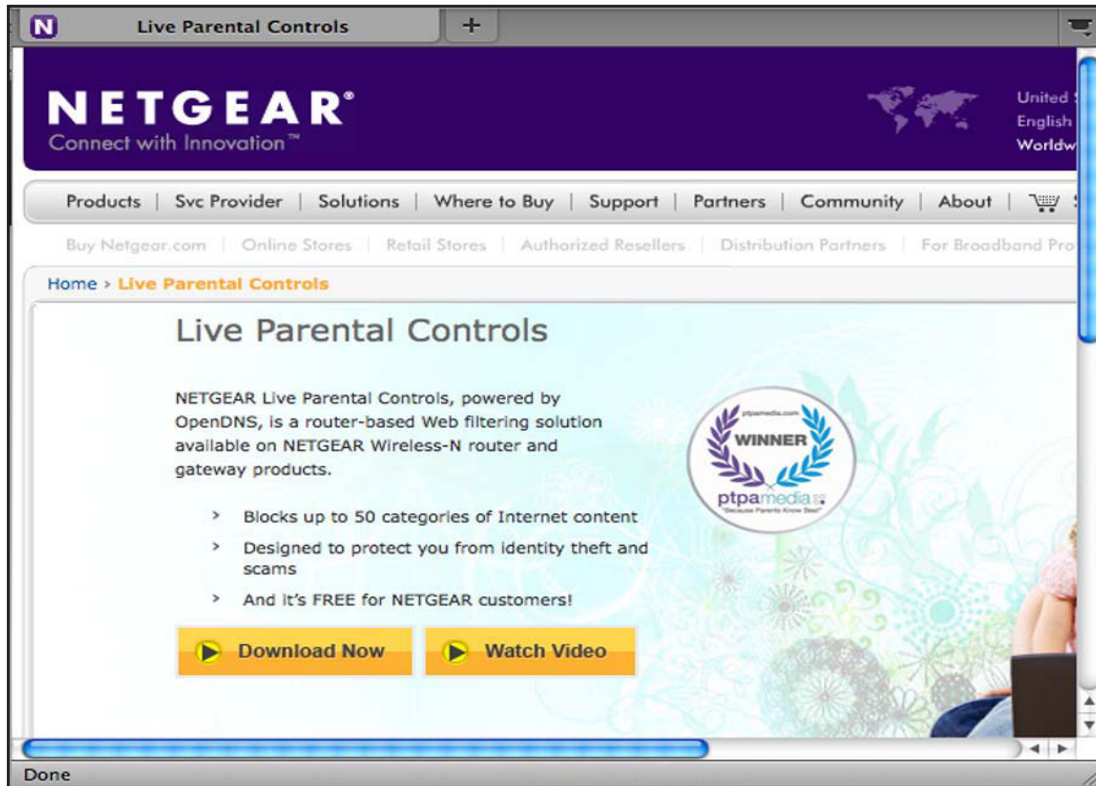
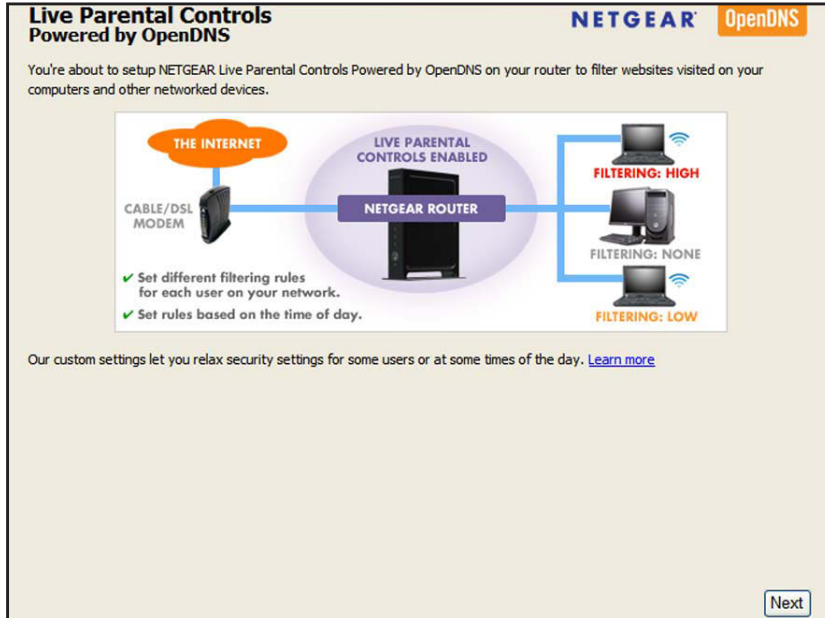


Figure 5. Live Parent Controls screen

➤ **To set up Live Parental Controls:**

1. On the Live Parental Controls screen, click either the **Windows Users** or **Mac Users** button.
2. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management Utility.

After installation, Live Parental Controls automatically starts.



- Click the **Next** button, read the note, and click the **Next** button again to proceed.

You are prompted to log in or create a free account.

Setting up Live Parental Controls

Welcome, this setup wizard will quickly configure NETGEAR Live Parental Controls Powered by OpenDNS on your NETGEAR router.

In order to use Live Parental Controls, you need a free OpenDNS account. Do you already have one?

☒ Yes, use my existing OpenDNS account.
☐ No, I need to create a free OpenDNS account.

- Select the radio button that applies to you and click the **Next** button.

Select one of the following:

- If you already have an OpenDNS account, leave the **Yes** radio button selected.
- If you do not have an OpenDNS account, select the **No** radio button. A screen displays that lets you set up a free OpenDNS account.

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

☐ **High**
Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, phishing attacks and general time-wasters.

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

☐ **Low**
Protects against pornography and phishing attacks.

☒ **Minimal**
Protects only against phishing attacks.

☐ **None**
Nothing blocked.

5. Select the radio button for the filtering level that you want and click the **Next** button.

Setup is complete!

You have successfully setup NETGEAR Live Parental Controls Powered by OpenDNS. Next time you run the Management Utility it will take you to the status screen where you can:

- check whether Live Parental Controls are enabled
- disable or enable Live Parental Controls
- modify basic settings
- change custom settings such as per-user and time-of-day based Live Parental Controls

[Take me to the status screen](#)

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

Parental controls are now set up for the router. The dashboard shows Parental Controls as enabled.

The next time that you select **Parental Controls** on the BASIC Home screen, you can sign in to your free OpenDNS account and manage the parental controls.

NETGEAR [Support](#) | [Sign in](#)

Parental Controls Center

Use OpenDNS Parental Controls with your router to make the Internet safer for your household.

Sign in to your OpenDNS account

Username

Password

[Sign in](#)

[Forgot your password?](#)

Important Note
If you have not yet configured the Live Parental Controls feature on your device please do so with the Management Utility found on the CD that came with your router or download it now for [Windows](#) or [Mac](#).

OpenDNS © 2012 OpenDNS

Figure 6. Sign in to your OpenDNS account screen

Guest Networks

Adding a guest network allows visitors at your home to use the Internet without using your wireless security key.

➤ **To set up a guest network:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > Guest Network**.

The 2.4 GHz and 5 GHz WiFi bands are configured separately.

3. To specify a guest network profile, in the Network Profiles section of the screen, select the radio button that is next to the profile that you want to use.
4. Enter the SSID in the **Name (SSID)** field.

The SSID is also known as the wireless network name. The default SSID is randomly generated. **NETGEAR recommends that you do not change the default SSID.** If you do decide to change the name, enter a 32-character (maximum) name in this field. This field is case-sensitive.

5. To enable the guest network, select the **Enable Guest Network** check box.

This feature allows guests to connect to your network using the SSID of this profile.

6. To enable SSID broadcast, select the **Enable SSID Broadcast** check box.

This feature allows the router to broadcast its SSID so that wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default, but you can clear it to disable broadcast of the SSID.

7. To allow guests to access your local network, select the **Allow guest to access My Local Network** check box.

This feature allows any user who connects to this SSID to have access to your local network, not just Internet access.

8. To enable wireless isolation, select the **Enable Wireless Isolation** check box.

This feature allows wireless clients (computers or wireless devices) that join the network to use the Internet, but they cannot access each other or access Ethernet devices on the network.

9. Specify the security option.

You can change the wireless authentication and encryption option and the password (also referred to as the wireless network password or network key). The security that you select encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network.



WARNING:

Do not disable wireless security!

The security options for your home wireless network and your guest wireless network are the same, but the wireless security key is different for each network. You can set up the security options for the guest network as discussed in the following sections:

- For information about how to set up WPA-PSK, WPA2-PSK, or WPA-PSK + WPA2-PSK mixed mode security, see [WPA-PSK, WPA2-PSK, and WPA-PSK + WPA2-PSK Mixed Mode](#) on page 28.
- For information about how to set up WPA/WPA2 enterprise security, see [WPA/WPA2 Enterprise](#) on page 29.
- For information about how to set up WEP security, see [WEP](#) on page 30.

Note: The **WEP** option displays only if you select **Up to 54 Mbps** from the **Mode** list.

10. Click the **Apply** button.

11. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:

- Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
- Does your wireless device or computer display on the Attached Devices screen? If it does, then it is connected to the network.
- If you are not sure what the SSID or password is, look on the label on your router.

FastLane

FastLane lets you reserve bandwidth when you are connecting from a trusted IP address. You can also specify whether the **WPS/FastLane** button on the router is used for WPS or FastLane. FastLane gives you guaranteed bandwidth for video streaming applications.

You can do the following:

- Turn on and off the FastLane feature. (FastLane is set to off by default.)
- Specify the IP address of the trusted computer.
- Set the **WPS/FastLane** button on your router to WPS or FastLane. (This button is set to WPS by default.)

➤ **To use FastLane:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > FastLane**.

The screenshot shows the 'FastLane' configuration page within the 'BASIC' settings tab. The left sidebar lists various settings categories, with 'FastLane' selected. The main content area has a title bar with 'FastLane' and 'Cancel'/'Apply' buttons. Below this, the 'FastLane Status' is set to 'Off'. There is a checkbox for 'Turn On FastLane'. The 'Trusted IP Address' field is set to '192.168.1.2'. Under 'WPS & FastLane Push Button', the 'WPS' radio button is selected, and the 'FastLane' radio button is unselected. At the bottom, there is a 'Help Center' link and a 'Show/Hide Help Center' button.

3. To enable FastLane, select the **Turn On FastLane** check box.
4. In the field provided, enter the IP address of the trusted computer.
When you connect to the router from the trusted IP address, you have guaranteed bandwidth for video streaming applications.
5. To specify FastLane for the **WPS/FastLane** button, select the **FastLane** radio button.
6. Click the **Apply** button.

4. genie ADVANCED Home

4

Specify custom settings

This chapter explains the advanced features of the router.

The chapter contains the following sections:

- [*Setup Wizard*](#)
- [*WPS Wizard*](#)
- [*WAN Setup*](#)
- [*LAN Setup*](#)
- [*Quality of Service Setup*](#)

Some selections on the ADVANCED Home screen are described in separate chapters:

- **Internet Setup.** This link is a shortcut to the same Internet Setup screen that you can access from the dashboard on the BASIC Home screen. See [*Internet Setup*](#) on page 24.
- **Wireless Setup.** This link is a shortcut to the same Wireless Settings screen that you can access from the dashboard on the BASIC Home screen. See [*Basic Wireless Settings*](#) on page 25.
- **Guest Network.** This link is a shortcut to the same Guest Network screen that you can access from the dashboard on the BASIC Home screen. See [*Guest Networks*](#) on page 36.
- **USB Storage.** See [*Chapter 5, USB Port*](#).
- **Security.** See [*Chapter 6, Security*](#).
- **Administration.** See [*Chapter 7, Administration*](#).
- **Advanced Setup.** See [*Chapter 8, Advanced Settings*](#).

Setup Wizard

The NETGEAR genie installation process is launched the first time you set up the router. After setting up the router the first time, if you want to perform this task again, you can run Setup Wizard from the ADVANCED tab of the genie.

➤ **To use the Setup Wizard:**

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

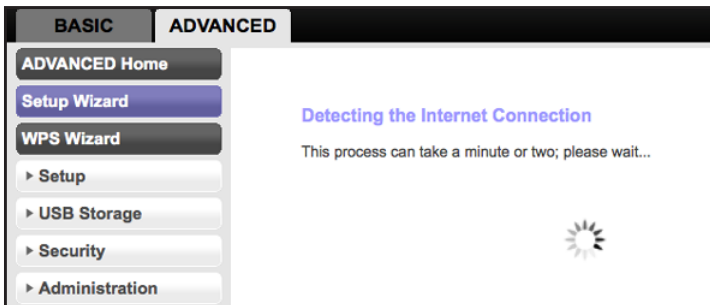
2. Select **Setup Wizard**.



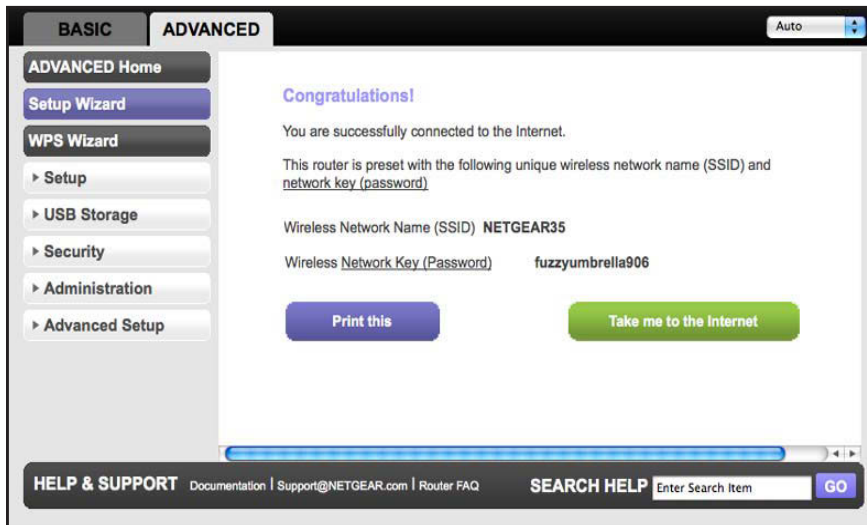
3. Select either the **Yes** or **No, I want to configure the router myself** radio button.

If you select the **No** button, you are taken to the Internet Setup screen. For more information, see [Internet Setup](#) on page 24.

4. If you selected the **Yes** button, click the **Next** button.



The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.



WPS Wizard

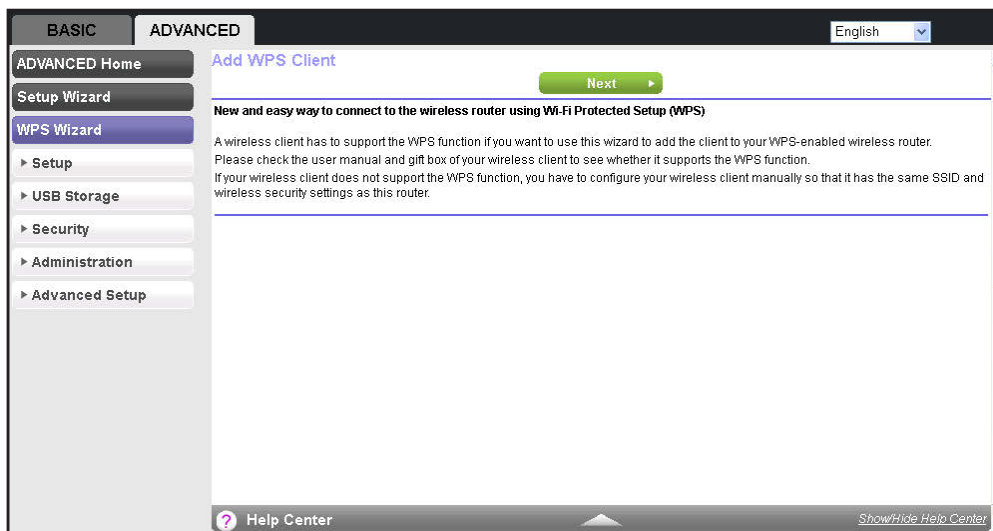
The WPS Wizard helps you add a WPS-capable client device (a wireless device or computer) to your network. On the client device, you need to either press its **WPS** button or locate its WPS PIN.

➤ To use the WPS Wizard:

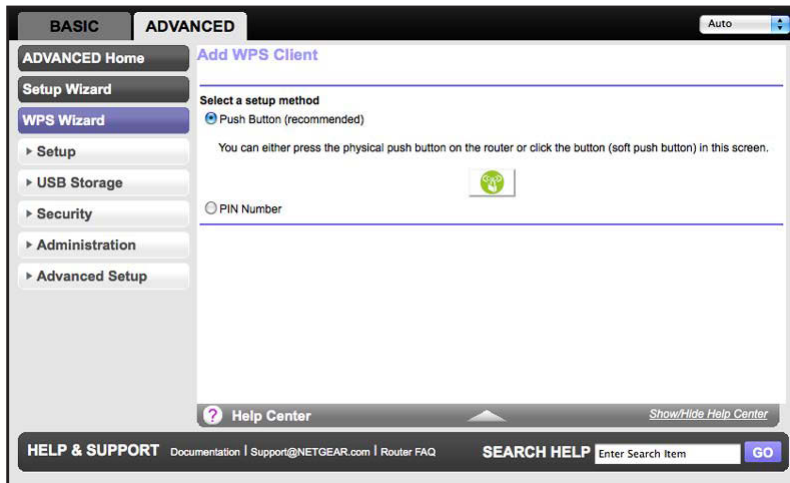
1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > WPS Wizard**.



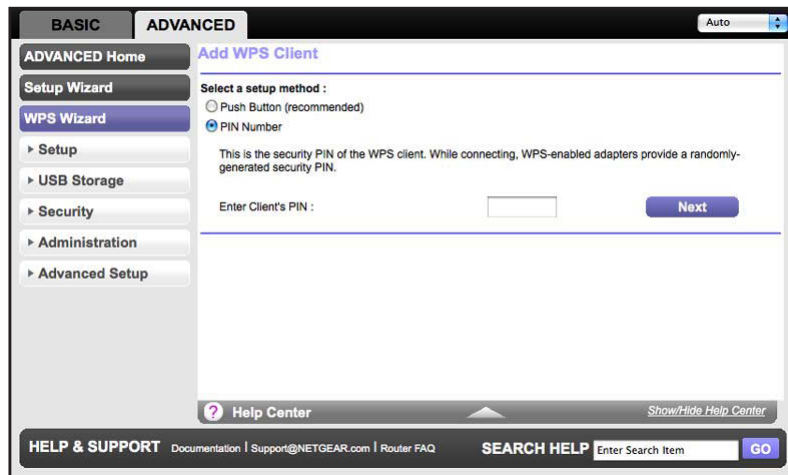
3. Click the **Next** button.



You can use either the push button or PIN method.

4. Select either the **Push Button** or **PIN Number** radio button.

- To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button on the side of the router. Within two minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.
- To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click the **Next** button.



Within two minutes, go to the client device and use its WPS software to join the network without entering a password.

The router attempts to add the WPS-capable device. The WPS LED on the front of the router blinks green. When the router establishes a WPS connection, the LED is solid green, and the router WPS screen displays a confirmation message.

5. Repeat [Step 2](#) through [Step 4](#) to add another WPS client to your network.

WAN Setup

You can configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the router to respond to a ping on the WAN (Internet) port. The router does not support a VPN endpoint, but it allows traffic from VPN endpoints to pass through.

➤ **To configure the WAN setup:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > WAN Setup**.

3. Enter the settings you want to customize:

- **Disable Port Scan and DoS Protection.** DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This check box should be selected only in special circumstances.
- **Default DMZ Server.** This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. For more information, see *Default DMZ Server* on page 44.
- **Respond to Ping on Internet Port.** If you want the router to respond to a ping from the Internet, select this check box. Use this capability only as a diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.
- **MTU Size (in bytes).** The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. This reduction is rarely required, and should not be done unless you are sure that it is necessary for your ISP connection. See *Change the MTU Size* on page 45.
- **NAT Filtering.** Network Address Translation (NAT) determines how the router processes inbound traffic:

- Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. By default, the **Secured** radio button is selected.
- Open NAT provides a much less secured firewall, but allows almost all Internet applications to function.
- **Disable SIP ALG.** Some Voice over IP (VoIP) applications do not function well with the Session Initiation Protocol (SIP) Application Layer Gateway (ALG). Selecting the check box to turn off the SIP ALG might enable connected VoIP devices to create and accept a VoIP call through the router. By default, this check box is cleared.
- **Disable IGMP Proxying.** IGMP proxying allows computers on the LAN to receive the multicast traffic they are subscribed to from the Internet. By default, this check box is selected, and the IGMP proxy is disabled, preventing multicast traffic from the Internet to the LAN. Clear the **Disable IGMP Proxying** check box to allow multicast traffic from the Internet to the LAN.
- **VPN Passthrough.** The router supports VPN passthrough for IPSec, PPTP, and L2TP.
 - **IPSec Passthrough.** To enable or disable IPSec passthrough, select the **Enable** or **Disabled** radio button.
 - **PPTP Passthrough.** To enable or disable PPTP passthrough, select the **Enable** or **Disabled** radio button.
 - **L2TP Passthrough.** To enable or disable L2TP passthrough, select the **Enable** or **Disabled** radio button.

4. Click the **Apply** button.

Default DMZ Server

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



WARNING:

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

Incoming traffic from the Internet gets discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Port

Forwarding/Port Triggering screen. Instead of discarding this traffic, you can forward it to one computer on your network. This computer is called the default DMZ server.

➤ **To set up a default DMZ server:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > WAN Setup**.

The screenshot shows the 'ADVANCED' tab selected, with 'WAN Setup' highlighted in the left sidebar. The main content area is titled 'WAN Setup' and includes a 'Cancel' button and an 'Apply' button. The 'Default DMZ Server' checkbox is checked, and the IP address 192.168.1.1 is entered. Other options include 'Disable Port Scan and DoS Protection', 'Respond to Ping on Internet Port', 'MTU Size' (set to 1500), 'NAT Filtering' (set to Secured), 'Disable SIP ALG', 'Disable IGMP Proxying', and 'VPN Passthrough' (with sub-options for IPSec, PPTP, and L2TP, all set to Enable).

3. Select the **Default DMZ Server** check box.
4. Type the IP address.
5. Click **Apply**.

Change the MTU Size

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has 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 just the default value, and changing the value might fix one problem but cause another. Leave the MTU unchanged unless one of these situations occurs:

- You have 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 have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

Note: An incorrect MTU setting can cause Internet communication problems such as the inability to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

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

Table 2. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size. This value is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for ping. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➤ **To change the MTU size:**

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

2. Select **ADVANCED > Setup > WAN Setup**.

3. In the **MTU Size** field, enter a new size from 64 through 1500.

4. Click **Apply**.

LAN Setup

You can configure LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

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

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

These addresses are part of the designated private address range for use in private networks and should be suitable for most applications. If your network requires the use of a different IP addressing scheme, make the changes in the LAN Setup screen.

Note: If you change the LAN IP address of the router while connected through the browser, you are disconnected. You must open a new connection to the new IP address and log in again.

➤ **To change the LAN settings:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > LAN Setup**.

The screenshot shows the 'LAN Setup' page in the router's web interface. The 'ADVANCED' tab is selected, and the 'LAN Setup' sub-tab is active. The 'Device Name' is set to 'JR6150'. Under 'LAN TCP/IP Setup', the 'IP Address' is '192.168.1.1', 'IP Subnet Mask' is '255.255.255.0', 'RIP Direction' is 'Both', and 'RIP Version' is 'Disabled'. The 'Use Router as DHCP Server' checkbox is checked. The 'Starting IP Address' is '192.168.1.2' and the 'Ending IP Address' is '192.168.1.254'. Below this is an 'Address Reservation' table with columns for '#', 'IP Address', 'Device Name', and 'MAC Address'. There are 'Add', 'Edit', and 'Delete' buttons for the table. A 'Help Center' link is at the bottom left, and a 'Show/Hide Help Center' link is at the bottom right.

3. Enter the following settings:

- **IP Address.** The LAN IP address of the router (by default, **192.168.1.1**).
- **IP Subnet Mask.** The LAN subnet mask of the router (by default, **255.255.255.0**). Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
- **RIP Direction.** Router Information Protocol (RIP) enables a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. **Both** is the default setting. With the **Both** or **Out Only** setting, the router broadcasts its routing table periodically. With the **Both** or **In Only** setting, the router incorporates the RIP information that it receives.
- **RIP Version.** This setting controls the format and the broadcasting method of the RIP packets that the router sends. It recognizes both formats when receiving. By default, the RIP function is disabled. Four RIP versions exist:
 - RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup.
 - RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
 - RIP-2B uses subnet broadcasting.
 - RIP-2M uses multicasting.

4. To set your computers' IP addresses manually, clear the **Use Router as DHCP Server** check box.

NETGEAR recommends that you do not do this. For more information, see [Use the Router as a DHCP Server](#) on page 49.

5. To reserve an IP address for a computer or device on the LAN, in the Address Reservation section, click the **Add** button.

For more information, see [Address Reservation](#) on page 50.

6. Click the **Apply** button.

Use the Router as a DHCP Server

By default, the router functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the router are satisfactory.

You can specify the pool of IP addresses for assignment by setting the starting IP address and ending IP address. These addresses must be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, define a range between 192.168.1.2 and 192.168.1.254, although you might want to save part of the range for devices with fixed addresses.

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

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

You can use another device on your network as the DHCP server or you can manually configure the network settings of all of your computers and devices.

➤ To disable the DHCP server feature:

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

2. Select **ADVANCED > Setup > LAN Setup**.

The screenshot shows the 'LAN Setup' page in the 'ADVANCED' tab of the router's web interface. The 'Device Name' is set to 'JR6150'. Under 'LAN TCP/IP Setup', the IP Address is 192.168.1.1, Subnet Mask is 255.255.255.0, RIP Direction is 'Both', and RIP Version is 'Disabled'. The 'Use Router as DHCP Server' checkbox is checked. The DHCP settings show a Starting IP Address of 192.168.1.2 and an Ending IP Address of 192.168.1.254. Below this is an 'Address Reservation' table with columns for #, IP Address, Device Name, and MAC Address. There are buttons for '+ Add', 'Edit', and 'Delete' for the reservation table. The left sidebar contains navigation links for 'BASIC', 'ADVANCED', 'Setup Wizard', 'WPS Wizard', 'Setup', 'Internet Setup', 'Wireless Setup', 'Guest Network', 'WAN Setup', 'LAN Setup' (highlighted), 'QoS Setup', 'USB Storage', 'Security', 'Administration', and 'Advanced Setup'. At the bottom, there is a 'Help Center' link and a 'Show/Hide Help Center' button.

3. Clear the **Use Router as DHCP Server** check box.

4. Click the **Apply** button.

If the DHCP service is not enabled on the router and no other DHCP server is available on your network, you must set your computers' IP addresses manually or your computers are not able to access the router.

Address Reservation

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

➤ **To reserve an IP address:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > LAN Setup**.

The screenshot shows the 'LAN Setup' page. The left sidebar has a 'Setup' section with 'LAN Setup' highlighted. The main content area has a 'Device Name' field with 'JR6150'. Under 'LAN TCP/IP Setup', there are fields for IP Address (192.168.1.1), IP Subnet Mask (255.255.255.0), RIP Direction (Both), and RIP Version (Disabled). There is a checkbox for 'Use Router as DHCP Server' which is checked. Below this are fields for Starting IP Address (192.168.1.2) and Ending IP Address (192.168.1.254). The 'Address Reservation' section contains a table with columns: #, IP Address, Device Name, and MAC Address. Below the table are buttons for '+ Add', 'Edit', and 'Delete'.

3. In the Address Reservation section, click the **Add** button.

The screenshot shows the 'Address Reservation' page. The left sidebar has 'LAN Setup' highlighted. The main content area has a title 'Address Reservation' and buttons for 'Refresh', 'Cancel', and 'Add'. Below is the 'Address Reservation Table' with one entry: #0, IP Address 192.168.1.2, Device Name MPAA LAN SPARE, and MAC Address 00:13:02:12:13:3F. Below the table are input fields for IP Address, MAC Address, and Device Name, and an 'Add' button.

4. In the **IP Address** field, type the IP address to assign to the computer or server.
Choose an IP address from the router's LAN subnet, such as 192.168.1.x.
5. Type the MAC address of the computer or server.

Tip: If the computer is already on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

6. Click the **Apply** button.

The reserved address is entered into the table.

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

Quality of Service Setup

You can use Quality of Service (QoS) to prioritize some types of traffic ahead of others. The router can provide QoS prioritization over the wireless link and on the Internet connection.

Wi-Fi Multimedia Quality of Service for Wireless Traffic

The router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS prioritizes wireless 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, both it and the client running that application need to have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS are assigned to the best effort category, which receives a lower priority than voice and video. WMM QoS is enabled by default.

Quality of Service Priority Rules and Internet Access

You can give prioritized Internet access to the following types of traffic:

- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the router
- A specific device by MAC address

To specify prioritization of traffic, you need to create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

By default, QoS is disabled for Internet traffic, the default QoS rules, and any custom QoS rules that you created are not activated, and no traffic is prioritized.

➤ To enable QoS for Internet traffic and activate the QoS rules:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > QoS Setup**.

3. Select the **Turn Internet Access QoS On** check box.

WMM QoS is enabled by default. NETGEAR recommends that you leave this setting as it is for full 802.11n wireless rate support.

4. To limit the bandwidth that is available for traffic from the router to the Internet, select the **Turn Bandwidth Control On** check box.

For more information, see [Bandwidth Control](#) on page 53.

5. Manage the QoS rules.

For more information about how to manage and create QoS rules, which are also referred to as QoS policies, see [Manage QoS Rules](#) on page 54.

6. To allocate half of the WAN bandwidth to a special host in heavy traffic situations, select the **Enable Trusted IP address** check box.

In the field that is provided, enter the IP address of the trusted host.

7. Click the **Apply** button.

Your settings are saved.

Bandwidth Control

Bandwidth control lets you set a limit to the bandwidth that is available for traffic from the router to the Internet.

➤ **To set the maximum uplink bandwidth:**

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

2. Select **ADVANCED > Setup > QoS Setup**.

3. Select the **Turn Bandwidth Control On** check box.
4. Select the **Automatically check Internet Uplink bandwidth** radio button.
5. Click the **Check** button.

The router detects the available uplink bandwidth. After about one minute, the available bandwidth displays on the screen. This information can help you to determine the maximum bandwidth setting that you want to allow.

6. Select the **Uplink bandwidth** radio button.
7. Enter the maximum bandwidth that you want to allow, and select either **Kbps** or **Mbps**.
8. Click the **Apply** button.

Manage QoS Rules

The following procedure refers to preconfigured and custom QoS rules, which are also referred to as QoS policies. For information about how to create custom QoS rules, see the sections following this section.

➤ **To view, change, or delete a QoS rule:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > QoS Setup**.

3. Click the **Set Up QoS Rule** button.

#	QoS Policy	Priority	Description
1	MSN Messenger	High	MSN Messenger Applications
2	Yahoo Messenger	High	Yahoo Messenger Applications
3	IP Phone	Highest	IP Phone Applications
4	Vonage IP Phone	Highest	Vonage IP Phone Applications
5	NetMeeting	High	NetMeeting Applications
6	AIM	High	AIM Applications
7	Google Talk	Highest	Google Talk Applications
8	Netgear EVA	Highest	Netgear EVA Applications
9	SSH	High	SSH Applications
10	Telnet	High	Telnet Applications
11	VPN	High	VPN Applications
12	FTP	Normal	FTP Applications
13	SMTP	Normal	SMTP Applications
14	WWW	Normal	WWW Applications
15	DNS	Normal	DNS Applications
16	eMule/eDonkey	Low	eMule/eDonkey Applications
17	Kazaa	Low	Kazaa Applications
18	Gnutella	Low	Gnutella Applications

All preconfigured QoS rules are displayed in a table, along with their priority (Highest, High, Normal, or Low) and a description.

4. Select the radio button next to the QoS policy that you want to edit or delete, and do one of the following:

- To remove the QoS policy from the table, click the **Delete** button.
- To edit the QoS policy, click the **Edit** button.

The QoS - Priority Rules screen displays.

- a. To change the policy settings, follow the instructions in the following sections:
 - [Create a QoS Rule for an Application or Online Game](#) on page 56
 - [Create a QoS Rule for Ethernet LAN Ports](#) on page 58
 - [Create a QoS Rule for a MAC Address](#) on page 59
- b. When you are done, on the QoS - Priority Rules screen, click the **Apply** button.
Your changes are saved in the table on the QoS Setup screen.

**WARNING:**

If you click the Delete All button, *all* preconfigured and custom QoS rules are deleted.

Create a QoS Rule for an Application or Online Game

- To create a QoS policy for an application or online game:

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

2. Select **ADVANCED** > **Setup** > **QoS Setup**.

The screenshot shows the 'QoS Setup' page in the 'ADVANCED' tab of the router's web interface. The left sidebar contains navigation links: 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup' (expanded), 'Internet Setup', 'Wireless Setup', 'WAN Setup', 'LAN Setup', 'QoS Setup' (selected), 'USB Storage', 'Security', 'Administration', and 'Advanced Setup'. The main content area has a 'QoS Setup' title and 'Cancel' and 'Apply' buttons. It includes checkboxes for 'Enable WMM (Wi-Fi multimedia) settings', 'Turn Internet Access QoS On', and 'Turn Bandwidth Control On'. Under 'Turn Bandwidth Control On', there are radio buttons for 'Uplink bandwidth Maximum' (set to 256 Kbps) and 'Automatically check Internet Uplink bandwidth', with a 'Check' button. Below this is a 'QoS Priority Rule list' section with a 'Set Up QoS Rule' button. At the bottom, there is a checkbox for 'Enable Trusted IP address' and a 'Trusted IP Address' field with four input boxes. The footer contains a 'Help Center' link and a 'Show/Hide Help Center' button.

3. Click the **Set Up QoS Rule** button.

QoS Priority Rule list

Cancel Apply

#	QoS Policy	Priority	Description
1	MSN Messenger	High	MSN Messenger Applications
2	Yahoo Messenger	High	Yahoo Messenger Applications
3	IP Phone	Highest	IP Phone Applications
4	Vonage IP Phone	Highest	Vonage IP Phone Applications
5	NetMeeting	High	NetMeeting Applications
6	AIM	High	AIM Applications
7	Google Talk	Highest	Google Talk Applications
8	Netgear EVA	Highest	Netgear EVA Applications
9	SSH	High	SSH Applications
10	Telnet	High	Telnet Applications
11	VPN	High	VPN Applications
12	FTP	Normal	FTP Applications
13	SMTP	Normal	SMTP Applications
14	WWW	Normal	WWW Applications
15	DNS	Normal	DNS Applications
16	eMule/eDonkey	Low	eMule/eDonkey Applications
17	Kazaa	Low	Kazaa Applications
18	Grutella	Low	Grutella Applications

Help Center Show/Hide Help Center

Edit Delete Delete All

+ Add Priority Rule

Help Center Show/Hide Help Center

Scroll down

4. Click the **Add Priority Rule** button.

QoS - Priority Rules

Cancel Apply

Priority

QoS Policy for MSN Messenger

Priority Category Applications

Applications MSN Messenger

Priority Normal

5. In the **Priority Category** list, select either **Applications** or **Online Gaming**:

- **Applications.** The **Applications** list lets you select existing applications, but scroll down to the bottom to select **Add a new application**.

QoS - Priority Rules

Cancel Apply

Priority

QoS Policy for

Priority Category Applications

Applications Add a new application

Priority Normal

Specified Port Range

Connection Type TCP/UDP

Starting Port (1-65535)

Ending Port (1-65535)

- **Online Gaming.** The **Online Gaming** list lets you select existing games, but scroll down to the bottom to select **Add a new game**.

6. In the **QoS Policy for** field, type a descriptive name for the new application or game.
7. From the **Priority** list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. Select **Highest**, **High**, **Normal**, or **Low**.
8. In the **Connection Type** field, select either **TCP**, **UDP**, or **TCP/UDP**.
9. In the **Starting Port** and **Ending Port** fields, specify the port number or range of port numbers that the application or game uses.
10. Click the **Apply** button.

The rule is saved in the QoS Policy table on the QoS Setup screen.

Create a QoS Rule for Ethernet LAN Ports

- To create a QoS policy for a device connected to one of the router's LAN ports:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > QoS Setup**.

3. Click the **Set Up QoS Rule** button.

QoS Priority Rule list

Cancel Apply

#	QoS Policy	Priority	Description
1	MSN Messenger	High	MSN Messenger Applications
2	Yahoo Messenger	High	Yahoo Messenger Applications
3	IP Phone	Highest	IP Phone Applications
4	Vonage IP Phone	Highest	Vonage IP Phone Applications
5	NetMeeting	High	NetMeeting Applications
6	AIM	High	AIM Applications
7	Google Talk	Highest	Google Talk Applications
8	Netgear EVA	Highest	Netgear EVA Applications
9	SSH	High	SSH Applications
10	Telnet	High	Telnet Applications
11	VPN	High	VPN Applications
12	FTP	Normal	FTP Applications
13	SMTP	Normal	SMTP Applications
14	WWW	Normal	WWW Applications
15	DNS	Normal	DNS Applications
16	eMule/Donkey	Low	eMule/Donkey Applications
17	Kazaa	Low	Kazaa Applications
18	Gnutella	Low	Gnutella Applications

Help Center Show/Hide Help Center

Edit Delete Delete All

+ Add Priority Rule

Help Center Show/Hide Help Center

Scroll down

4. Click the **Add Priority Rule** button.

QoS - Priority Rules

Cancel Apply

Priority

QoS Policy for MSN Messenger

Priority Category Applications

Applications MSN Messenger

Priority Normal

5. In the **Priority Category** list, select **Ethernet LAN Port**.

QoS - Priority Rules

Cancel Apply

Priority

QoS Policy for LAN Port 1

Priority Category Ethernet LAN Port

LAN Port 1

Priority Normal

6. In the **QoS Policy for** field, type a descriptive name for the LAN port.
7. From the **LAN Port** list, select the LAN port number.
8. From the **Priority** list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. Select **Highest**, **High**, **Normal**, or **Low**.
9. Click the **Apply** button.

The rule is saved in the QoS Policy table on the QoS Setup screen.

Create a QoS Rule for a MAC Address

- To create a QoS policy for traffic from a specific MAC address:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > QoS Setup**.

The screenshot shows the 'QoS Setup' page in the router's web interface. The left sidebar contains a navigation menu with 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', and a 'Setup' section with sub-items: 'Internet Setup', 'Wireless Setup', 'WAN Setup', 'LAN Setup', 'QoS Setup' (highlighted), 'USB Storage', 'Security', 'Administration', and 'Advanced Setup'. The main content area is titled 'QoS Setup' and includes a 'Cancel' button and an 'Apply' button. It has several checkboxes: 'Enable WMM (Wi-Fi multimedia) settings' (checked), 'Turn Internet Access QoS On' (unchecked), and 'Turn Bandwidth Control On' (unchecked). Under 'Turn Bandwidth Control On', there are radio buttons for 'Uplink bandwidth Maximum' (selected) and 'Automatically check Internet Uplink bandwidth'. The 'Uplink bandwidth Maximum' option has a value of '256' and a unit of 'Kbps'. There is a 'Check' button. Below these is a 'QoS Priority Rule list' section with a 'Set Up QoS Rule' button. At the bottom, there is a 'Trusted IP address' section with a checkbox 'Enable Trusted IP address' and a 'Trusted IP Address' field. A 'Help Center' link is at the bottom left, and a 'Show/Hide Help Center' link is at the bottom right.

3. Click the **Set Up QoS Rule** button.

The screenshot shows the 'QoS Priority Rule list' table. The table has four columns: '#', 'QoS Policy', 'Priority', and 'Description'. It lists 18 rules, each with a radio button in the first column. The rules are as follows:

#	QoS Policy	Priority	Description
1	MSN Messenger	High	MSN Messenger Applications
2	Yahoo Messenger	High	Yahoo Messenger Applications
3	IP Phone	Highest	IP Phone Applications
4	Vonage IP Phone	Highest	Vonage IP Phone Applications
5	NetMeeting	High	NetMeeting Applications
6	AIM	High	AIM Applications
7	Google Talk	Highest	Google Talk Applications
8	Netgear EVA	Highest	Netgear EVA Applications
9	SSH	High	SSH Applications
10	Telnet	High	Telnet Applications
11	VPN	High	VPN Applications
12	FTP	Normal	FTP Applications
13	SMTP	Normal	SMTP Applications
14	WWW	Normal	WWW Applications
15	DNS	Normal	DNS Applications
16	eMule/eDonkey	Low	eMule/eDonkey Applications
17	Kazaa	Low	Kazaa Applications
18	Gnutella	Low	Gnutella Applications

Below the table is a 'Help Center' link. At the bottom of the page, there are buttons for 'Edit', 'Delete', 'Delete All', and 'Add Priority Rule' (highlighted). A 'Show/Hide Help Center' link is also present. An arrow points from the 'Add Priority Rule' button to the next screenshot.

4. Click the **Add Priority Rule** button.

The screenshot shows the 'QoS - Priority Rules' dialog box. It has a 'Cancel' button and an 'Apply' button. The dialog contains the following fields:

- Priority**: A dropdown menu with 'Applications' selected.
- QoS Policy for**: A text input field with 'MSN Messenger' entered.
- Priority Category**: A dropdown menu with 'MSN Messenger' selected.
- Applications**: A dropdown menu with 'Normal' selected.

5. In the **Priority Category** list, select **MAC Address**.

QoS - Priority Rules

Cancel Apply

Priority
QoS Policy for
Priority Category: MAC Address

	QoS Policy	Priority	Device Name	MAC Address
☐	Pri_MAC_12133F	Normal	MPAWLAN-SPARE	00:13:02:12:13:3F

MAC Address
Device Name
Priority: Normal

+ Add Edit Delete Refresh

6. In the **QoS Policy for** field, type a descriptive name for the MAC address.

7. If the device for which you want to create a QoS policy is displayed in the MAC Device List, select its radio button.

The information from the MAC Device List populates the policy name, **MAC Address**, and **Device Name** fields.

8. (Optional) If the device does not display in the MAC Device List, click the **Refresh** button.

If it still does not display, you must complete these fields manually.

9. From the **Priority** list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. Select **Highest**, **High**, **Normal**, or **Low**.

10. Click the **Apply** button.

The rule is saved in the QoS Policy table on the QoS Setup screen.

➤ **To edit or delete a MAC address on the MAC Device List:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Setup > QoS Setup**.

BASIC ADVANCED Auto

ADVANCED Home
Setup Wizard
WPS Wizard
Setup
Internet Setup
Wireless Setup
WAN Setup
LAN Setup
QoS Setup
USB Storage
Security
Administration
Advanced Setup

QoS Setup

Cancel Apply

☒ Enable WMM (Wi-Fi multimedia) settings

☐ Turn Internet Access QoS On

☐ Turn Bandwidth Control On

Uplink bandwidth Maximum: 256 Kbps

☐ Automatically check Internet Uplink bandwidth Check

QoS Priority Rule list Set Up QoS Rule

☐ Enable Trusted IP address

Trusted IP Address

Help Center Show/Hide Help Center

3. Click the **Set Up QoS Rule** button.

QoS Priority Rule list

Cancel Apply

#	QoS Policy	Priority	Description
☐ 1	MSN Messenger	High	MSN Messenger Applications
☐ 2	Yahoo Messenger	High	Yahoo Messenger Applications
☐ 3	IP Phone	Highest	IP Phone Applications
☐ 4	Vonage IP Phone	Highest	Vonage IP Phone Applications
☐ 5	NetMeeting	High	NetMeeting Applications
☐ 6	AIM	High	AIM Applications
☐ 7	Google Talk	Highest	Google Talk Applications
☐ 8	Netgear EVA	Highest	Netgear EVA Applications
☐ 9	SSH	High	SSH Applications
☐ 10	Telnet	High	Telnet Applications
☐ 11	VPN	High	VPN Applications
☐ 12	FTP	Normal	FTP Applications
☐ 13	SMTP	Normal	SMTP Applications
☐ 14	WWW	Normal	WWW Applications
☐ 15	DNS	Normal	DNS Applications
☐ 16	eMule/Donkey	Low	eMule/Donkey Applications
☐ 17	Kazaa	Low	Kazaa Applications
☐ 18	Gnutella	Low	Gnutella Applications

Help Center Show/Hide Help Center

Edit Delete Delete All

+ Add Priority Rule

Help Center Show/Hide Help Center

Scroll down

4. Click the **Add Priority Rule** button.

QoS - Priority Rules

Cancel Apply

Priority

QoS Policy for MSN Messenger

Priority Category Applications

Applications MSN Messenger

Priority Normal

5. In the **Priority Category** list, select **MAC Address**.

QoS - Priority Rules

Cancel Apply

Priority

QoS Policy for

Priority Category MAC Address

MAC Device List

	QoS Policy	Priority	Device Name	MAC Address
☐	Pri_MAC_12133F	Normal	MPAWLAN-SPARE	00:13:02:12:13:3F

MAC Address

Device Name

Priority Normal

+ Add Edit Delete Refresh

6. Select the radio button next to the device that you want to edit or delete, and do one of the following:

- To remove the device from the table, click the **Delete** button.
- To edit the MAC address, device name, or priority:
 - Click the **Edit** button.
 - Edit the information you want to change.

Note: *You cannot delete or edit a device that is detected and automatically added to the MAC Device List.*

7. Click the **Apply** button.

The device information is saved or removed from the MAC Device List.

5. USB Port

5

Enhance your local network

This chapter describes how to use the USB port on your router to enhance your local network.

The chapter contains the following sections:

- *Enhance Your Local Network*
- *Set Up Network Storage*
- *Access and Share Your Network Storage*
- *Set Up a Network Printer*

Enhance Your Local Network

Find the USB port on your router.



Figure 7. USB port

You can use the USB port for any of the following applications:

- **Network storage.** Back up the files on your computers and digital devices to a network drive. For more information, see [Set Up Network Storage](#) on page 66.
- **ReadySHARE Access.** Share the files on your network drive with local and remote computers and digital devices. For more information, see [Access and Share Your Network Storage](#) on page 75.
- **ReadySHARE Printer.** Send the files on your computers and digital devices to a network printer. For more information, see [Set Up a Network Printer](#) on page 79.

The USB port on the router can connect only USB devices such as flash drives or USB hard drives, and USB printers.

Do not connect computers, USB modems, USB hubs, CD drives, or DVD drives to the router's USB port.

Set Up Network Storage

You can back up the files on your local computers and digital devices to a network drive. ReadySHARE lets you access and share a USB drive connected the router's USB port.

The router works with most USB-compliant external flash and hard drives. If your USB device requires nonstandard drivers, it is not compatible. For the most up-to-date list of USB drives supported by the router, visit <http://kbserver.netgear.com/readysware>.

Connect or Safely Remove a USB Drive

The router supports both read and write for FAT16, FAT32, NTFS, and Linux file systems (EXT2 and EXT3). Some USB external hard drives and flash drives require drivers to be loaded into the Windows computer before the Windows computer can access the USB device. Such USB devices do not work with the router.

To physically disconnect a USB drive from the router USB port, first log in to the router and then safely remove it.

➤ To connect a USB storage device:

1. Insert your USB storage device into the USB port of the router.

For information about how to locate the USB port, see [Enhance Your Local Network](#) on page 65.

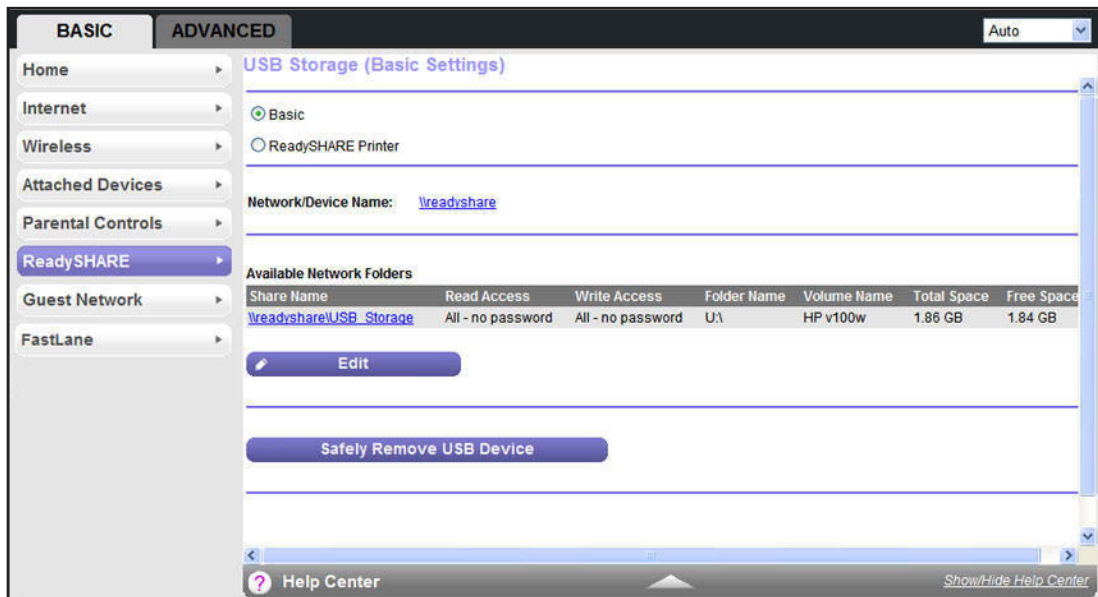
2. If your USB device has a power supply, connect the power supply to a power source.
It might take up to two minutes before the USB device is ready for sharing.

➤ To remove a USB disk drive safely:

1. Log in to the router.

For more information, see [Use NETGEAR genie After Installation](#) on page 27.

2. Select **BASIC > ReadySHARE**.



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

This action takes the drive offline.

4. Physically disconnect the USB drive.

View or Configure a USB Drive

You can view or configure your USB storage device:

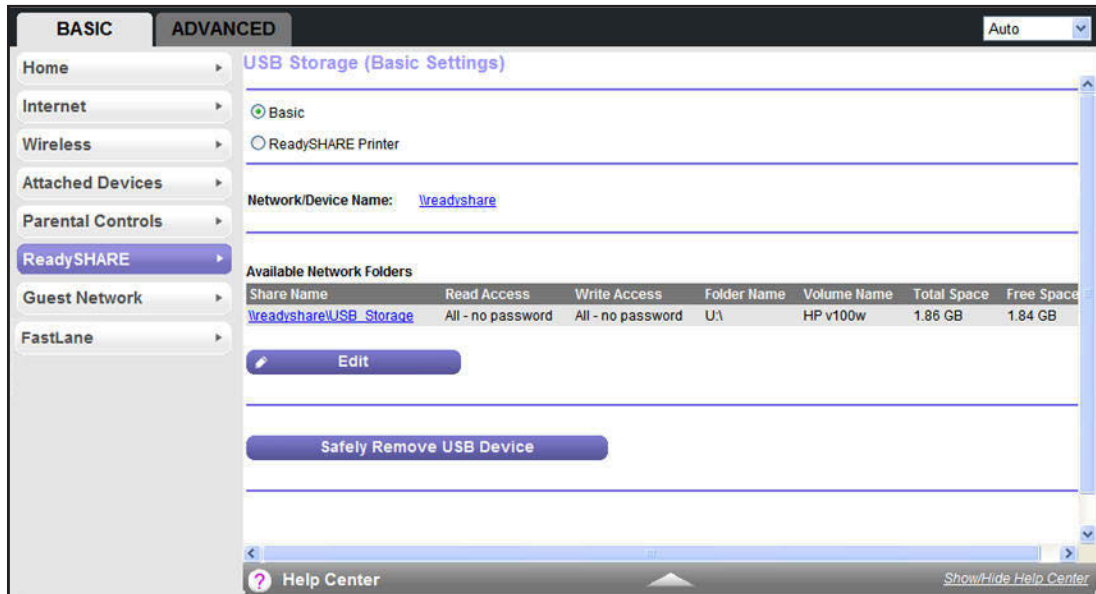
- View the basic information about the drive.
- Set up the device name, workgroups, and network folders.
- View or change the network folders.
- For more security, share only approved USB devices.

➤ **To view basic information about the USB storage device:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > ReadySHARE**.



The screen displays a USB storage device if it is attached to the router USB port.

If you logged in to the router before you connected your USB device, you might not see your USB device in this screen. If this happens, log out and log back in.

3. To view the files and folders on the USB device, click the network device name or the share name.
4. To view more detail or to change the USB device settings, click the **Edit** button.

The USB Storage (Advanced Settings) screen displays. For more information, see *Configure the USB Storage Device and Access Settings* on page 68.

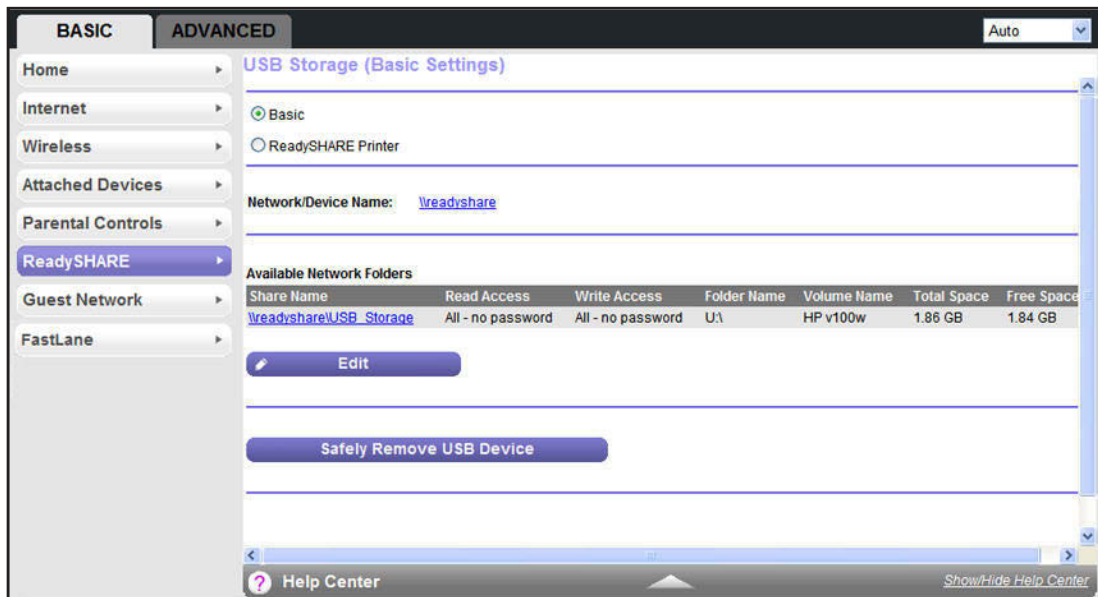
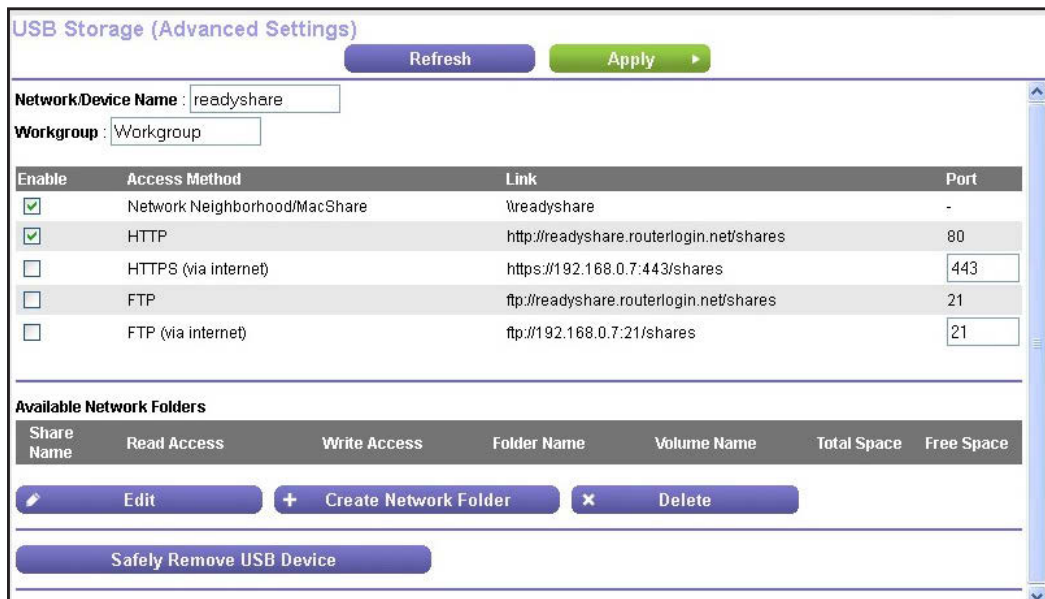
Configure the USB Storage Device and Access Settings

You can set up the device name, workgroups, and network folders for your USB device.

➤ **To view or change the USB storage advanced settings:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > ReadySHARE**.3. Click the **Edit** button.

4. To specify access to the USB storage device, provide the following information:

- **Network Device Name.** The default is **readyshare**. This name is the name used to access the USB device connected to the router.
- **Workgroup.** If you are using a Windows workgroup rather than a domain, the workgroup name displays here. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows.
- **Access Method.** Select the check boxes for the access methods that you want:
 - **Network Neighborhood/MacShare.** Enabled by default.

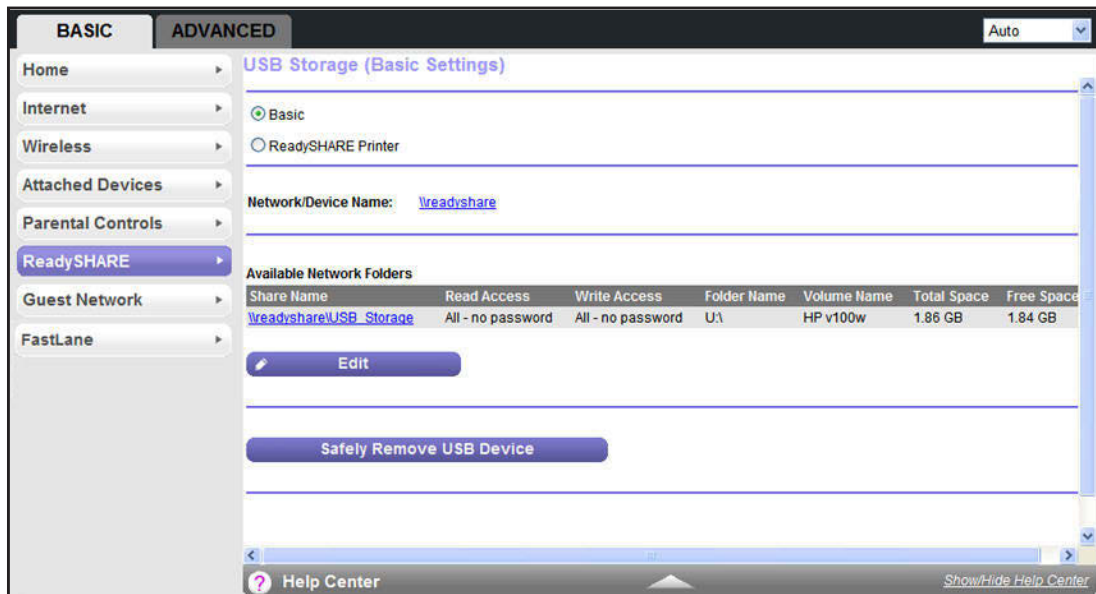
- **HTTP**. Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB drive.
 - **HTTP (via Internet)**. Disabled by default. If you enable this feature, remote users can type **http://<public IP address>/shares** (for example, **http://1.1.10.102/shares**) or a URL domain name to access the USB drive over the Internet. This feature supports file uploading only.
 - **FTP**. Disabled by default.
 - **FTP (via Internet)**. Disabled by default. If you select this check box, remote users can access the USB drive through FTP over the Internet. This feature supports both downloading and uploading of files.
5. If you changed the settings, click the **Apply** button.
Your changes are saved.

Configure the Available Network Folders

You can view or change the network folders on the USB storage device.

➤ **To view network folders:**

1. Log in to the router.
For more information, see *Use NETGEAR genie after Installation* on page 17.
2. Select **BASIC > ReadySHARE**.



3. Click the **Edit** button.

USB Storage (Advanced Settings)

Refresh Apply

Network/Device Name : readyshare

Workgroup : Workgroup

Enable	Access Method	Link	Port
☒	Network Neighborhood/MacShare	\\readyshare	-
☒	HTTP	http://readyshare.routerlogin.net/shares	80
☐	HTTPS (via internet)	https://192.168.0.7:443/shares	443
☐	FTP	ftp://readyshare.routerlogin.net/shares	21
☐	FTP (via internet)	ftp://192.168.0.7:21/shares	21

Available Network Folders

Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
Edit Create Network Folder Delete						

Safely Remove USB Device

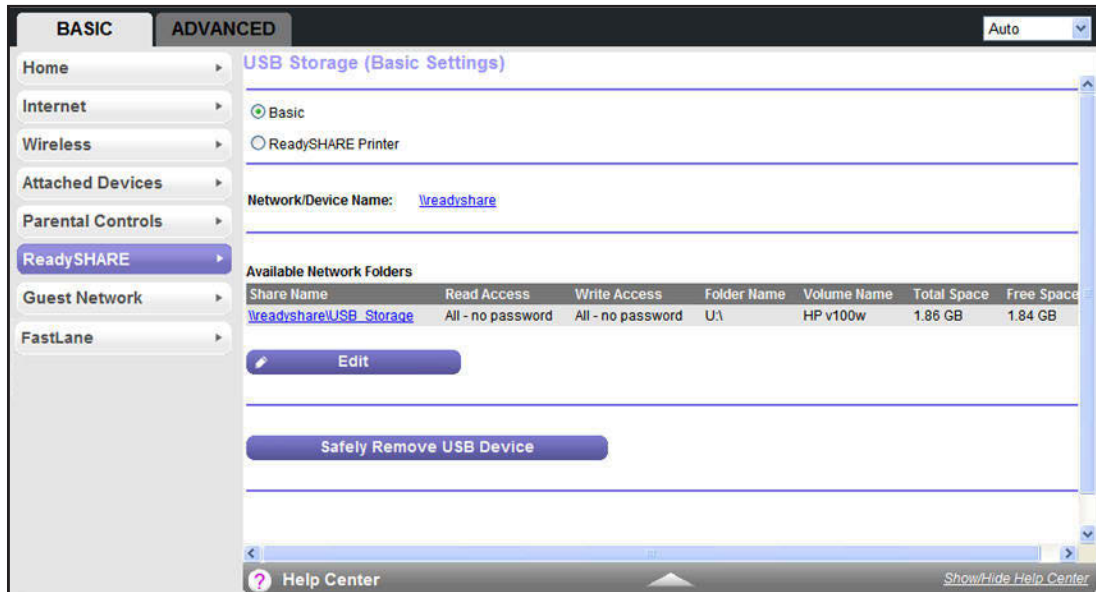
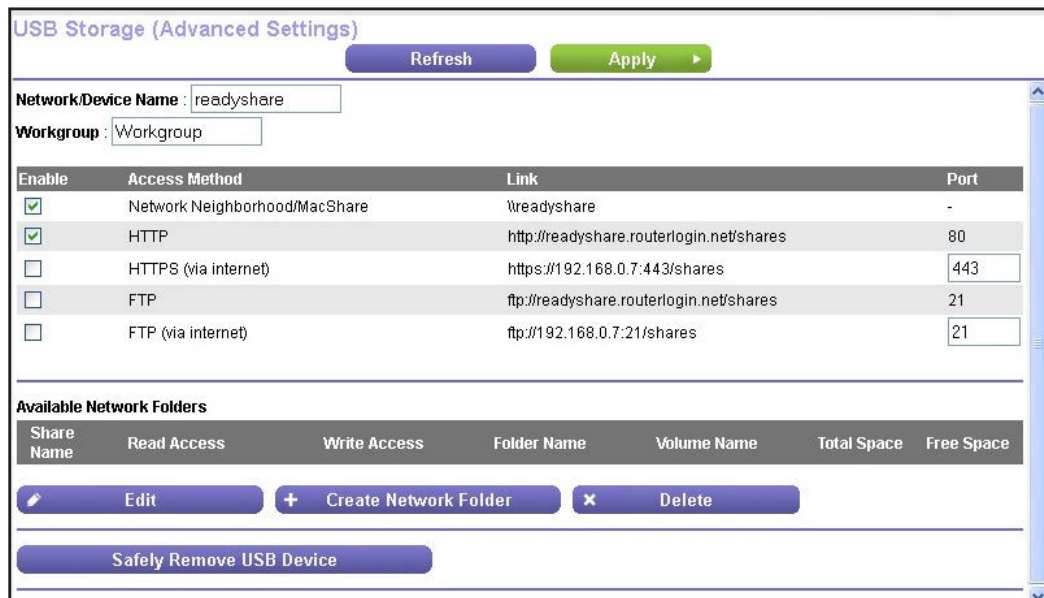
4. Scroll down to the Available Networks Folder section of the screen. The following information displays:

- **Share Name.** If only one device is connected, the default share name is USB_Storage. (Some router models have more than one USB port.)
You can click the name, or you can type it in the address field of your web browser. If Not Shared is shown, the default share was deleted and no other share for the root folder exists. Click the link to change this setting.
- **Read Access and Write Access.** Show the permissions and access controls on the network folder. All – no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the router.
- **Folder Name.** Full path of the network folder.
- **Volume Name.** Volume name from the storage device (either USB drive or HDD).
- **Total Space and Free Space.** Show the current utilization of the storage device.

➤ **To add a network folder:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **BASIC > ReadySHARE**.3. Click the **Edit** button.

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

http://www.routerlogin.net/USB_Folder_creat.htm

Create Network Folder

USB Device: U:\ Drive (1.96 GB)

Folder: [Browse](#)

Share Name:

Read Access: All - no password

Write Access: All - no password

[Apply](#)

[Close Window](#)

If the Create a Network Folder screen does not display, your web browser might be blocking pop-ups. If it is, change the browser settings to allow pop-ups.

- Click the **Browse** button next to the **Folder** field, and select the folder.
- Enter a name in the **Share Name** field.
- In the **Read Access** list and the **Write Access** list, select the settings that you want.

The user name (account name) for All – no password is guest. The password for admin is the same one that is used to log in to the router. By default, it is password.

- Click the **Apply** button.

The folder is added on the USB device.

➤ **To edit a network folder:**

- Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

- Select **BASIC > ReadySHARE**.

BASIC ADVANCED Auto

Home Internet Wireless Attached Devices Parental Controls ReadySHARE Guest Network FastLane

USB Storage (Basic Settings)

☒ Basic ☐ ReadySHARE Printer

Network/Device Name: readyshare

Available Network Folders

Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
readyshare\USB_Storage	All - no password	All - no password	U:\	HP v100w	1.96 GB	1.84 GB

[Edit](#)

[Safely Remove USB Device](#)

Help Center Show/Hide Help Center

3. Click the **Edit** button.

USB Storage (Advanced Settings)

Refresh Apply

Network/Device Name : readyshare

Workgroup : Workgroup

Enable	Access Method	Link	Port
☒	Network Neighborhood/MacShare	\\readyshare	-
☒	HTTP	http://readyshare.routerlogin.net/shares	80
☐	HTTPS (via internet)	https://192.168.0.7:443/shares	443
☐	FTP	ftp://readyshare.routerlogin.net/shares	21
☐	FTP (via internet)	ftp://192.168.0.7:21/shares	21

Available Network Folders

Share Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
Edit + Create Network Folder x Delete Safely Remove USB Device						

4. Click the **Edit** button.

The Edit Network Folder screen displays the same settings shown in the Create a Network Folder screen.

5. Change the settings in the fields as needed.
6. Click the **Apply** button.

Your changes are saved.

Specify Approved USB Devices

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

➤ To set up approved USB devices:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

USB Settings

Apply

Enable any USB Device connected to the USB port ☒ Yes ☐ No Approved Devices

- Click the **Approved Devices** button.

USB Drive Approved Devices

Refresh Apply

☐ Allow only approved devices

Approved USB Devices

Volume Name	Device Name	Capacity
Delete		

Available USB Devices

Volume Name	Device Name	Capacity
HP v100w	HP v100w	1.86 GB

Add

This screen shows the approved USB devices and the available USB devices.

- In the Available USB Devices list, select the drive that you want to approve.
- Click the **Add** button.
- Select the **Allow only approved devices** check box.
- Click the **Apply** button.

Your change takes effect.

If you want to work with another USB device, first click the **Safely Remove USB Device** button for the currently connected USB device and physically remove the device. Connect the other USB device and repeat this process. For more information, see [Connect or Safely Remove a USB Drive](#) on page 66.

Access and Share Your Network Storage

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be Windows, Mac, or Linux file types (NTFS, FAT32, HFS+, Ext 3, Ext 4), including text, Word, PowerPoint, Excel, MP3, picture, and multimedia files.

Common Uses of Network Sharing

USB drive applications include the following:

- Sharing multimedia such as MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network. You can store files in a central location so that you do not need to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and Windows computers by using the USB drive as a go-between across the systems.
- Sharing large files such as Word documents, PowerPoint presentations, and text files with remote users.

Share Photos and Multimedia

You can create your own central storage location for photos and multimedia. This method eliminates the need to log in to (and pay for) an external photo-sharing site.

➤ To share photos and multimedia with your friends and family:

1. Insert your USB drive into the USB port on the router either directly or with a USB cable.
Computers on your local area network (LAN) can automatically access this USB drive using a web browser or Microsoft Networking.
2. If you want to specify read-only access or to allow access from the Internet, see *Configure the USB Storage Device and Access Settings* on page 68.

Print High-Quality Photos from a Non-Shared Printer

You can print high-quality photos from a non-shared printer. This scenario is for a family that does not have a print server:

- A family member has photos on a Macintosh computer and wants to print them.
- The photo-capable color printer is directly attached to a Windows computer, but not shared on the network.
- The Mac and the Windows computer are not visible to each other on the network.

➤ To print high-quality photos from a non-shared printer:

1. On the Mac, access the USB drive by typing `\\readyshare` in the address field of a web browser. Then copy the photos to the USB drive.
2. On a Window computer, use a web browser or Microsoft Networking to copy the files from the USB drive to the computer. Then print the files.

You can also set up a network printer. For more information, see *Set Up a Network Printer* on page 79.

Send Large Files over the Internet

Sending files that are larger than 5 MB can pose a problem for many email systems. The router allows you to share large files such as PowerPoint presentations or .zip files over the Internet. You can use FTP to download shared files from the router.

Sharing files with a remote colleague involves the following considerations:

- The two user accounts are admin and guest. The password for admin is the same one that you use to access the router. By default, it is password. The guest user account has no password.
- On the FTP site, the person receiving the files uses the guest user account and enters the password. FTP requires that you type something in the password field.
- Be sure to select the **FTP (via Internet)** check box in the USB Storage (Advanced Settings) screen. This option supports both downloading and uploading of files.

Note: You can select the **HTTP (via Internet)** check box on the USB Storage (Advanced Settings) screen to share large files. This option supports downloading files only.

For more information, see [Access Your USB Storage Device Remotely](#) on page 78.

Access Your USB Storage Device Locally

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

➤ **To access the USB device from a local Mac computer:**

1. Select **Go > Connect to Server**.
2. Enter **smb://readyshare** as the server address.
3. Click the **Connect** button.

➤ **To access the USB device from a local Windows computer:**

Use any of these methods:

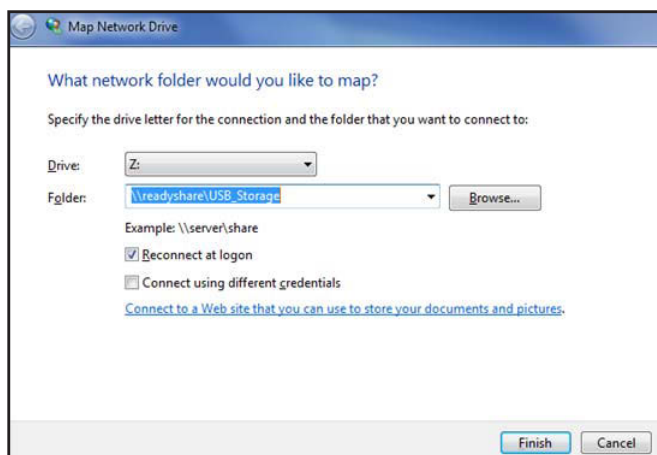
- Select **Start > Run**. Enter **\\readyshare** in the dialog box and click the **OK** button.
- Open a browser and enter **\\readyshare** in the address bar.
- Open My Network Places and enter **\\readyshare** in the address bar.

➤ **To map the USB device to a local Windows network drive:**

1. Visit www.netgear.com/readyshare.
2. In the ReadySHARE USB Storage Access pane, click the **PC Utility** button.

The `readyshareconnect.exe` file is downloaded to your computer.

3. Launch `readyshareconnect.exe`.



4. Select the drive letter that you want to map to the network folder.
5. If you want to connect to the USB drive as a different user, select the **Connect using different credentials** check box.
 - a. Type the user name and password that you want to use.
 - b. Click the **OK** button.
6. Click the **Finish** button.

The USB drive is mapped to the drive letter that you specified.

Access Your USB Storage Device Remotely

When you connect the USB device to the router USB port, it might take up to two minutes before it is ready for sharing. You can access your USB storage device remotely.

➤ To access the USB drive from a remote computer:

1. Launch a web browser.
2. Connect using the router's Internet port IP address.

If you are using Dynamic DNS, you can type the DNS name rather than the IP address. You can view the router's Internet IP address on the BASIC Home screen. For more information, see *BASIC Home Screen* on page 16).

➤ To access the USB drive with FTP from a remote computer:

1. Make sure that the **FTP** check box is selected in the Access Method section of the USB Storage (Advanced Settings) screen.

For more information, see *Configure the USB Storage Device and Access Settings* on page 68.

2. Launch a web browser.
3. Type **ftp://** and the Internet port IP address in the address field of the browser.

For example, type **ftp://10.1.65.4**.

If you are using Dynamic DNS, you can type the DNS name rather than the IP address.

4. Type the account name and password for the account that has access rights to the USB drive.

The user name (account name) for All – no password is **guest**.

The directories of the USB drive that your account has access to display. For example, you could see `share/partition1/directory1`. You can now read and copy files from the USB directory.

➤ To access the USB drive with ReadySHARE access from the Internet:

You can access your USB device in any of the following ways:

- On Windows 7, Windows 8, Windows XP, Windows Vista, and Windows 2000 systems, select **Start > Run**, and enter **\\readyshare** in the dialog box. Click the **OK** button.
- On Windows 7, Windows 8, Windows XP, Windows Vista, and Windows 2000 systems, open Internet Explorer, or Safari, and enter **\\readyshare** in the address bar.
- On Mac OS X (version 10.2 or later), enter **smb://readyshare** in the address bar.
- In My Network Places, enter **\\readyshare** in the address bar.

For more information about ReadySHARE access for USB storage devices, visit <http://www.netgear.com/readyshare>.

Set Up a Network Printer

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

You must install this utility before you can use the ReadySHARE Printer feature. For this feature to work, the following conditions must be met:

- This utility must be installed and running in the background on each computer from which you want to control this USB printer.
- The driver software for the USB printer must be installed on each computer from which you want to control this USB printer.

The ReadySHARE Printer utility has both a Mac version and a Windows version. The ReadySHARE Printer utility setup file and instructions are available by visiting www.netgear.com/readyshare. After you install the ReadySHARE Printer utility, it displays on your computer as the NETGEAR USB Control Center.

➤ To set up ReadySHARE Printer:

1. Using a USB printer cable, connect a USB printer to the router's USB port.

For information about how to locate the USB port, see [Enhance Your Local Network](#) on page 65.

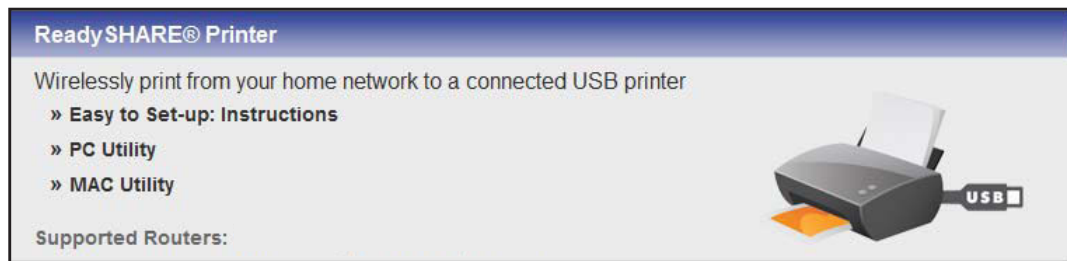
2. Install the USB printer driver software *on each computer* that shares the printer.

If you do not have the printer driver, contact the printer manufacturer.

3. On each computer that shares the printer, download the NETGEAR USB Control Center utility.

The NETGEAR USB utility has a Mac version and a Windows version, which you can access in two different ways:

- From the ReadySHARE Printer area of the page you access from www.netgear.com/readyspace.



- From the ReadySHARE section of the desktop NETGEAR genie.
For more information, see [NETGEAR genie App and Mobile genie App](#) on page 18.

Note: You must install this utility before you can use the ReadySHARE Printer feature. For the ReadySHARE Printer feature to work, this utility must be running in the background.

4. Follow the instructions to install the NETGEAR USB Control Center utility.

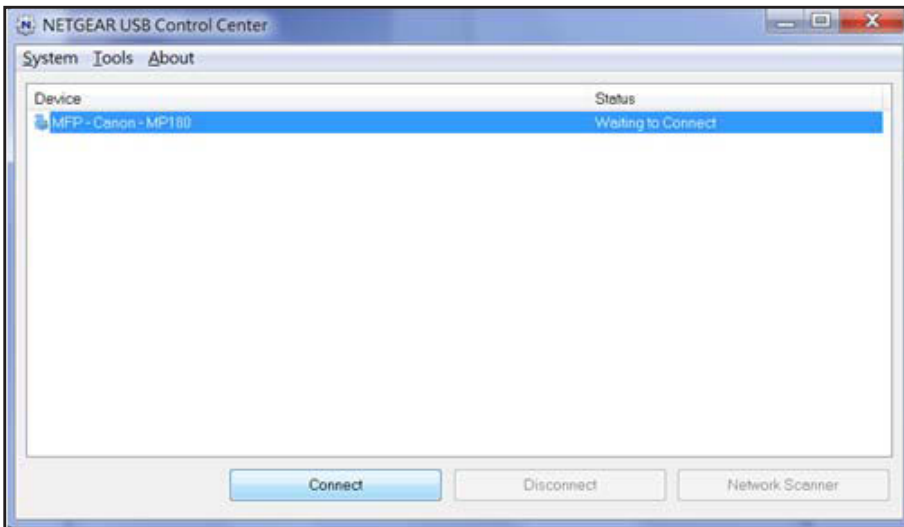


5. After you install the utility, select the language.

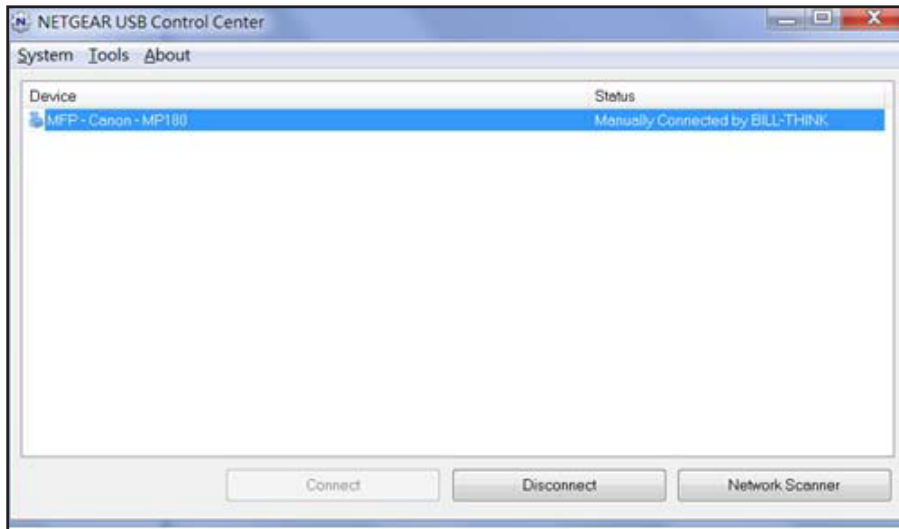


If this setup is the first time you are accessing the utility, you are asked to select the printer.

6. Click the **Connect** button.

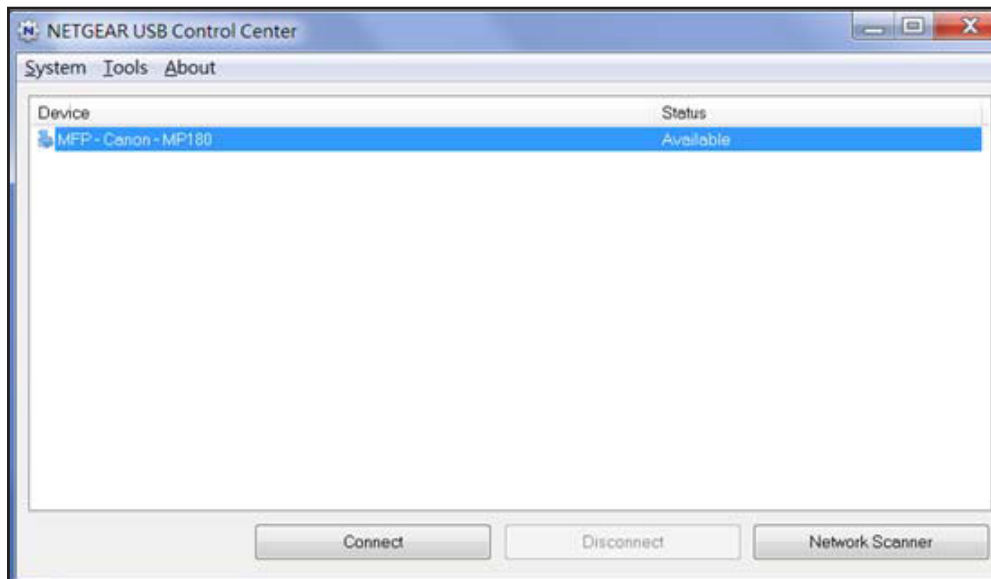


Once the connection is established, the status changes to Manually connected by xxx.



7. Click the **Disconnect** button at any time to release the connection.

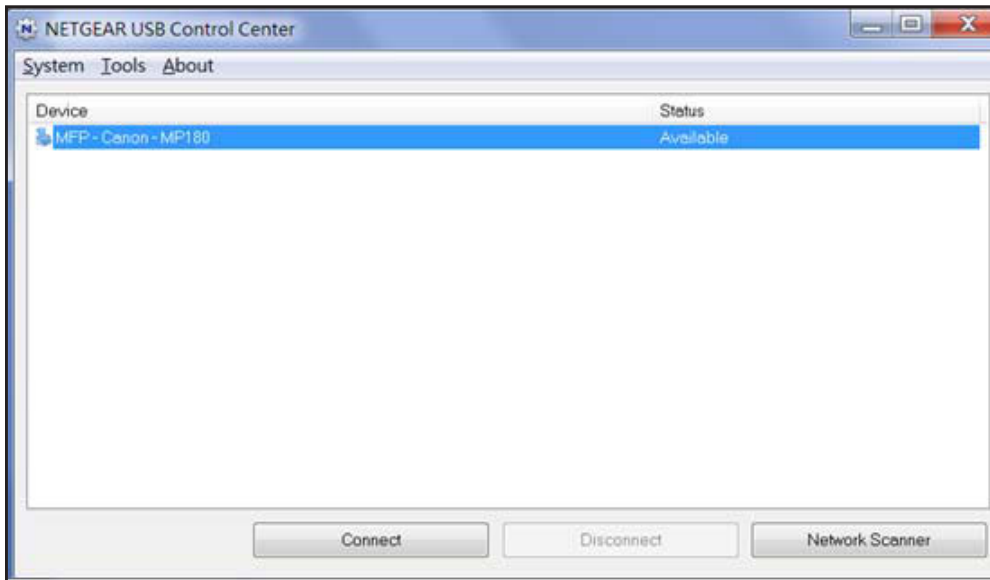
The status then changes to Available.



For each computer, after you click the **Connect** and **Disconnect** buttons once, the utility automatically handles the printing queue. The status of the printer displays as Available on all the computers. Here are the rules of operation:

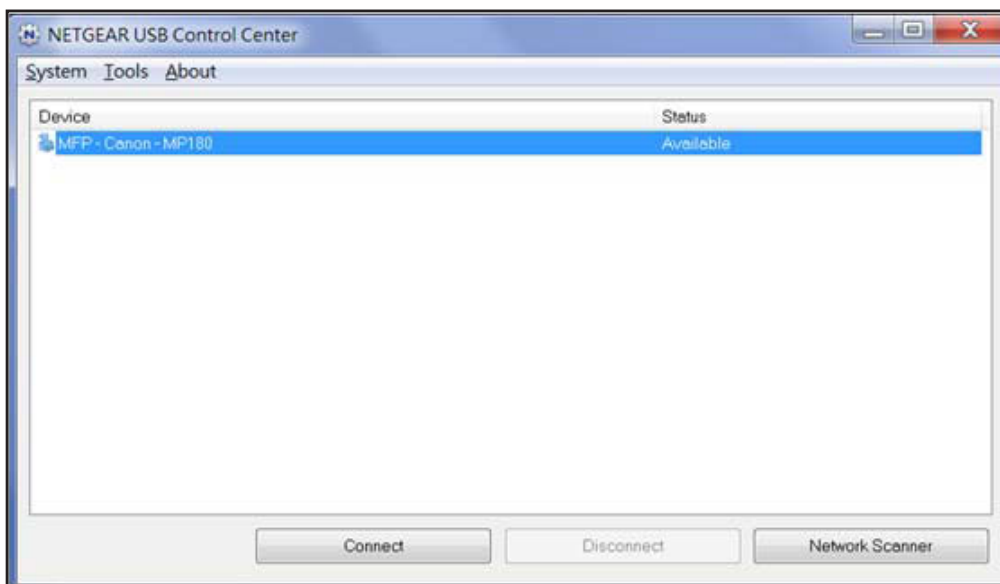
- When the status is Available, you can use the USB printer.
- When the status is Manually connected by xxx, only the xxx computer can use the printer. Other network devices must wait until the xxx computer has released the connection, or until the connection times out (the default time-out value is 30 seconds).

- You can set the value for the default time-out time from the Control Center - Configuration screen.



- The USB Control Center utility must be running for the computer to print to the USB printer attached to the router. If you exit the utility, printing does not work.
- Some firewall software, such as Comodo, blocks the ReadySHARE Print utility from accessing the USB printer. If you do not see the printer in the utility, you can disable the firewall temporarily to allow the utility to work.
- If your printer supports scanning, make sure that the printer is in the Available state and click the **Network Scanner** button.

This step activates the scanner window so you can use the printer for scanning.



6. Security

6

Keep unwanted content out of your network

This chapter explains how to use the basic firewall features of the router to prevent objectionable content from reaching the computers and other devices connected to your network.

The chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Port Filtering to Block Services*
- *Schedule Blocking*
- *Security Event Email Notifications*

For information about parental controls, see *Parental Controls* on page 33.

For information about access control, see *Set Up a Wireless Access List by MAC Address* on page 110.

Keyword Blocking of HTTP Traffic

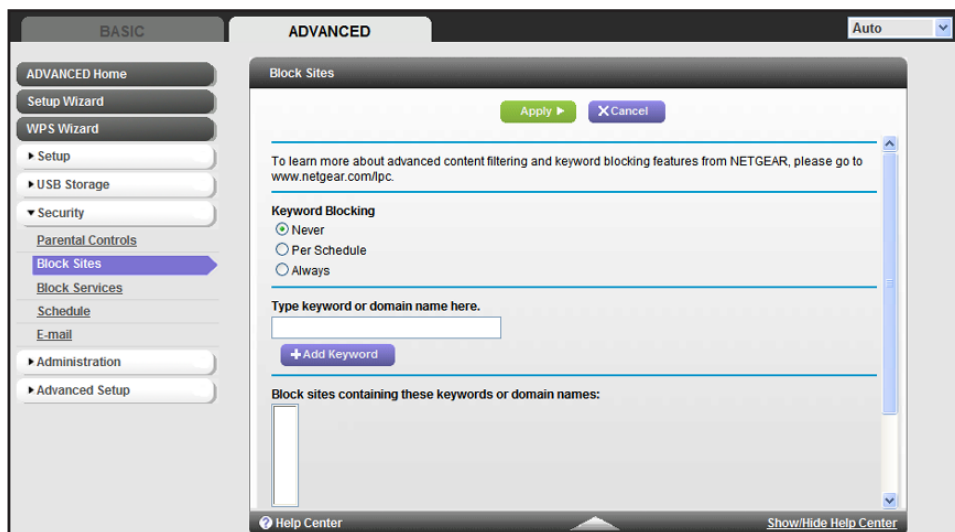
Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a schedule.

➤ **To configure keyword blocking:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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



3. Select one of the keyword blocking options:
 - **Per Schedule.** Turn on keyword blocking according to the Schedule screen settings.
 - **Always.** Turn on keyword blocking all the time, independent of the Schedule screen.
4. In the **keyword** field, enter a keyword or domain, click **Add Keyword**, and click **Apply**.

The keyword list supports up to 32 entries. Here are some sample entries:

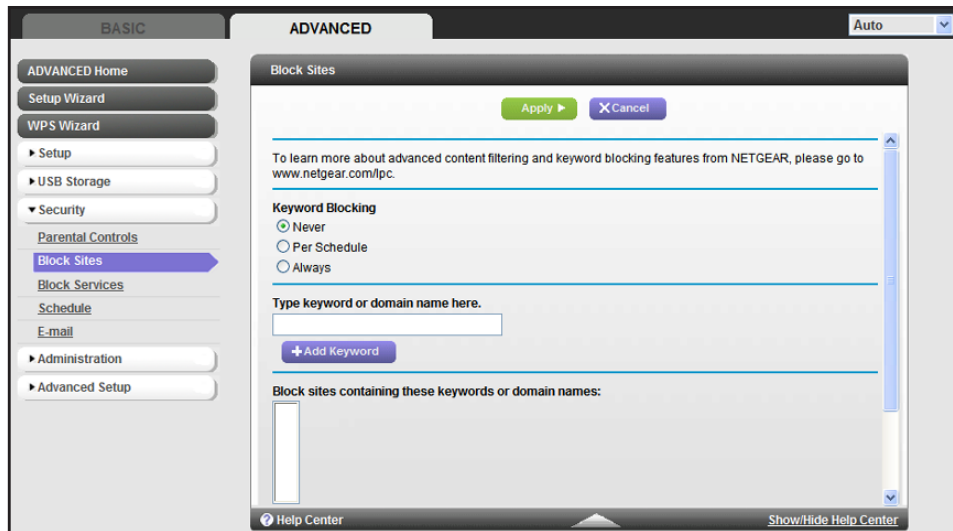
- Specify XXX to block <http://www.badstuff.com/xxx.html>.
- Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
- Enter a period (.) to block all Internet browsing access.

➤ **To delete a keyword or domain:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

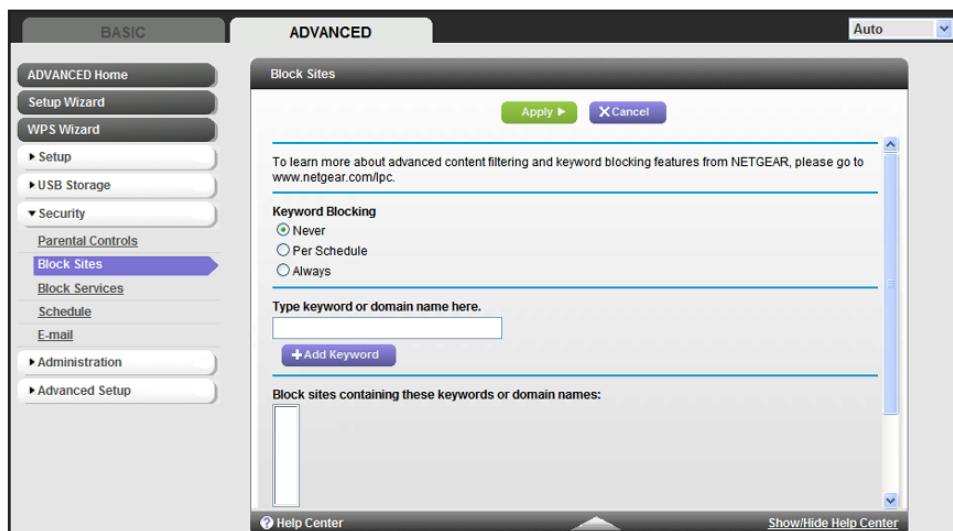


3. Select the keyword you want to delete from the list.
4. Click the **Delete Keyword** button.
5. Click the **Apply** button.

You can exempt one trusted computer from blocking and logging. The computer you exempt must have a fixed IP address.

➤ **To specify a trusted computer:**

1. Log in to the router.
For more information, see *Use NETGEAR genie after Installation* on page 17.
2. Select **ADVANCED > Security > Block Sites**.



3. In the **Trusted IP Address** field, enter the IP address.
4. Click the **Apply** button.

Port Filtering to Block Services

Services are functions performed by server computers at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service gets identified by a service or port number. This 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 <http://www.ietf.org/>) and published in RFC1700, "Assigned Numbers." The authors of other applications typically choose service numbers for those applications from the range 1024–65535. Although the router already holds a list of many service port numbers, you are not limited to these choices. You can often find port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

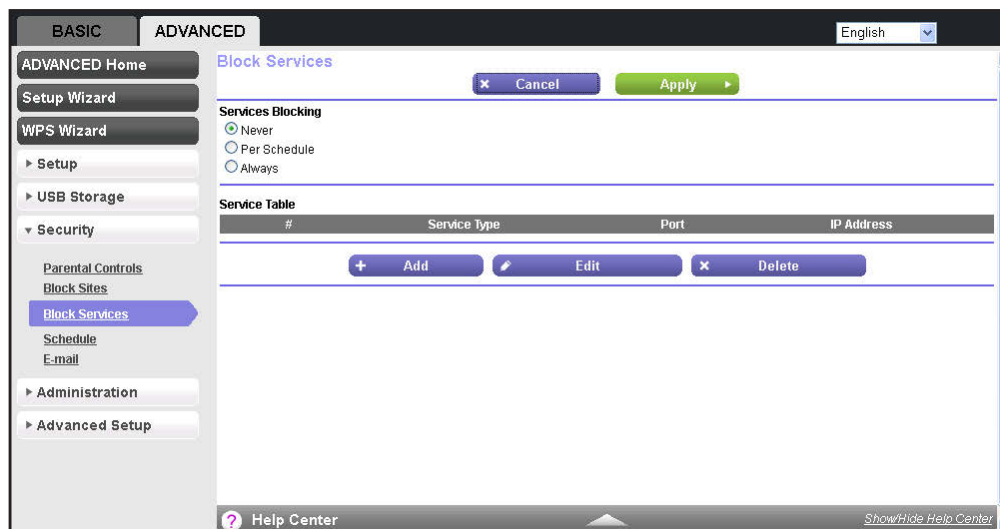
You can add and block specific Internet services by computers on your network. This process is called service blocking or port filtering. To add a service for blocking, first determine which port number or range of numbers the application uses.

➤ To block services:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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



3. Select either the **Per Schedule** radio button or the **Always** radio button.
4. If you selected **Per Schedule**, specify a time period in the Schedule screen.

For more information, see *Schedule Blocking* on page 88.

5. To add a service, click the **Add** button.

Block Services Setup

Cancel Add

Service Type: User Defined

Protocol: TCP

Starting Port: (1~65535)

Ending Port: (1~65535)

Service Type/User Defined

Filter Services For :

☐ Only This IP Address: 192.168.1.1

☐ IP Address Range: 192.168.1.1 to 192.168.1.1

☒ All IP Addresses

6. From the **Service Type** list, select the application or service to block.

The list displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.

7. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **TCP/UDP** (both).
8. Enter the starting and ending port numbers.

If the application uses a single port number, enter that number in both fields.

9. Select the radio button for the IP address configuration you want to block and enter the IP addresses.

You can block the specified service for a single computer, a range of computers with consecutive IP addresses, or all computers on your network.

10. Click the **Add** button.

Your changes are saved.

Schedule Blocking

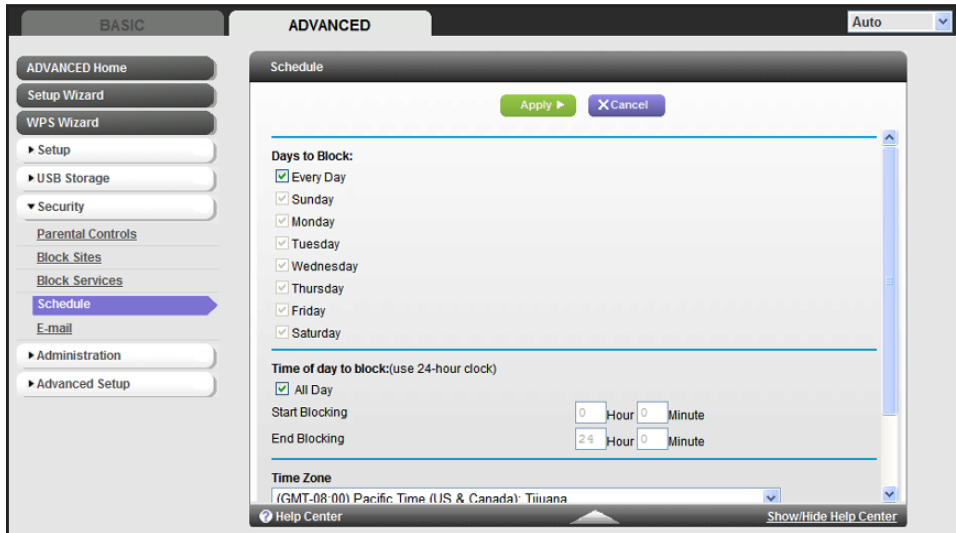
You can specify the days and time that you want to block Internet access.

➤ To schedule blocking:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Security > Schedule**.



3. Set up the schedule for blocking keywords and services. Here is what you can choose:
- **Days to Block.** Select days on which you want to apply blocking by selecting the appropriate check boxes, or select the **Every Day** check box to select the check boxes for all days.
 - **Time of Day to Block.** Select a start and end time in 24-hour format, or select the **All Day** check box for 24-hour blocking.
4. Select your time zone from the list. If you use daylight saving time, select the **Automatically adjust for daylight savings time** check box.
5. Click the **Apply** button.

Your settings are saved.

Security Event Email Notifications

You can receive logs and alerts by email and specify which alerts you want to receive and how often.

➤ **To set up email notifications:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

3. Select the **Turn Email Notification On** check box.
4. In the **Your Outgoing Mail Server** field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com).

You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages are not sent.

5. Enter the email address to which logs and alerts are sent in the **Send to This E-mail Address** field.

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

6. To use a secure connection, select the **Secure connection (use SSL)** check box.
7. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box.

Complete the **User Name** and **Password** fields for the outgoing email server.

8. Select the **Send Alerts Immediately** check box.

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

9. Enter the information in the fields in the Send logs according to this schedule section of the screen.

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

10. Click the **Apply** button.

Your settings are saved.

Administration

7

Manage your network

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

The chapter includes the following sections:

- [*View Router Status*](#)
- [*View Logs of Web Access or Attempted Web Access*](#)
- [*Manage the Configuration File*](#)
- [*Upgrade the Router Firmware*](#)

Some information for administering and maintaining your router and local network are described in separate chapters:

- For information about changing and recovering your password, see [*Change the Password*](#) on page 18 and [*Password Recovery*](#) on page 19.
- For information about the devices that are connected to your network, see [*Attached Devices*](#) on page 32.
- For information about upgrading or checking the status of your router over the Internet, see [*Remote Management*](#) on page 136.
- For information about monitoring the volume of Internet traffic passing through your router's Internet port, see [*Traffic Meter*](#) on page 139.

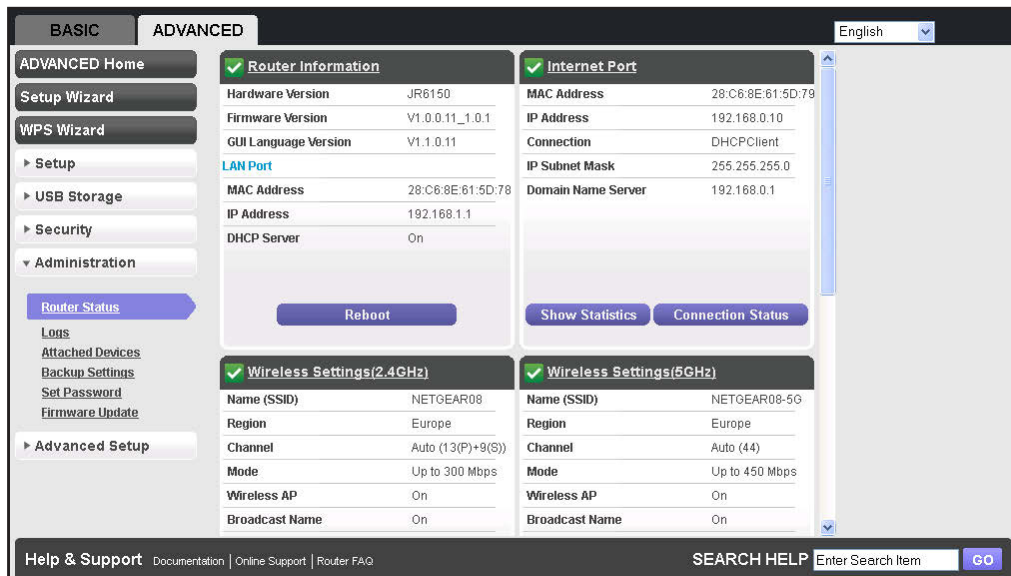
View Router Status

➤ To view router status and usage information:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Click the **ADVANCED** tab.



Note: The Router Status screen also displays when you select **ADVANCED > Advanced Home** or **ADVANCED > Administration > Router Status**.

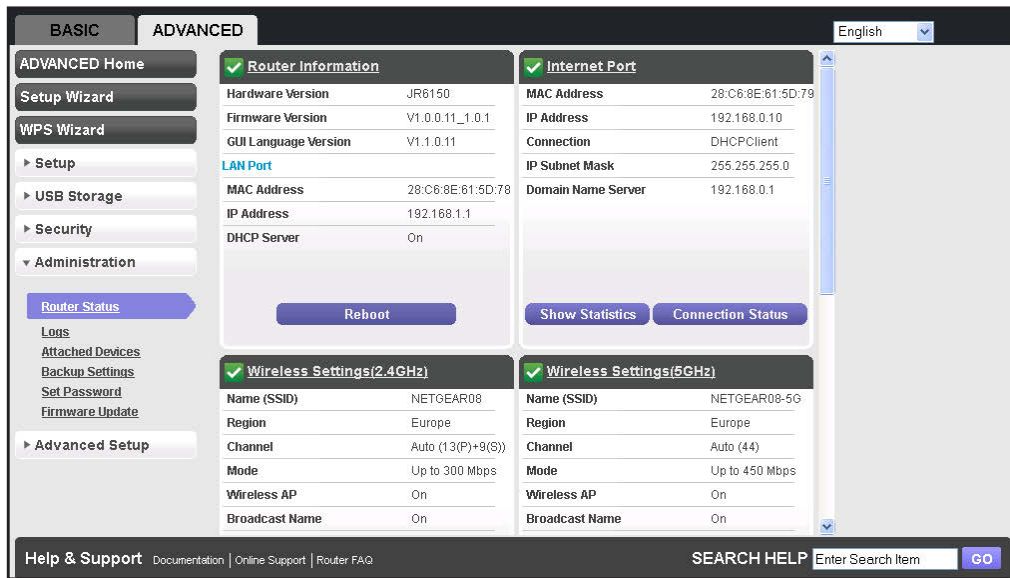
Router Information Pane

➤ To display the Router Information pane:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Click the **ADVANCED** tab.



The following information displays:

- **Hardware Version.** The router model.
- **Firmware Version.** The version of the router firmware. It changes if you upgrade the router firmware.
- **GUI Language Version.** The localized language of the router user interface.
- **LAN Port:**
 - **MAC Address.** The Media Access Control address for the LAN port. This address is the unique physical address that the Ethernet (LAN) port of the router uses.
 - **IP Address.** The IP address that the Ethernet (LAN) port of the router uses. The default is 192.168.1.1.
 - **DHCP Server.** Identifies whether the router's built-in DHCP server is active for the LAN-attached devices.

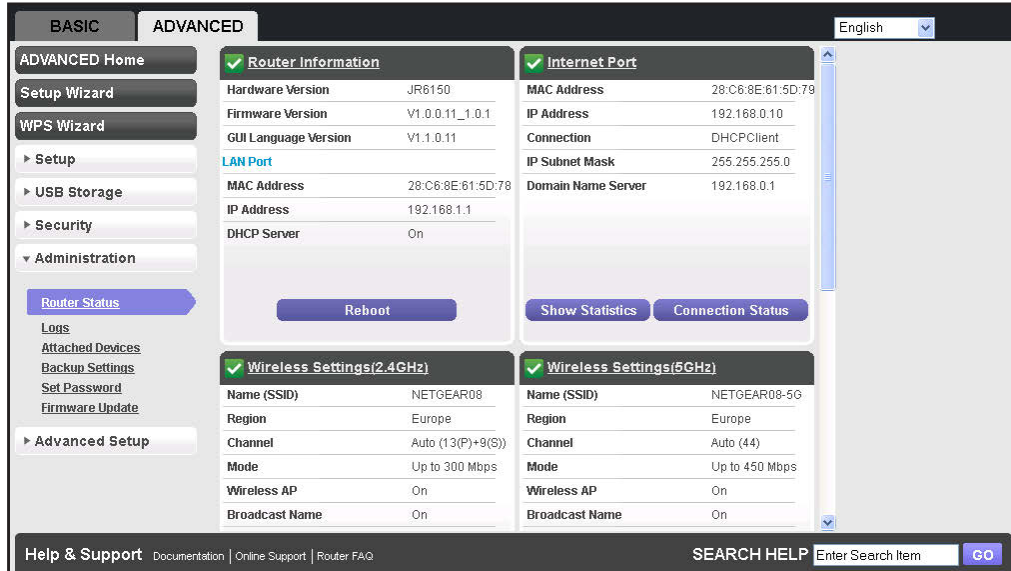
Internet Port Pane

➤ **To display the Internet Port pane:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Click the **ADVANCED** tab.



The following information displays:

- **MAC Address.** The Media Access Control (MAC) address for the Internet port. This address is the unique physical address that the Internet (WAN) port of the router uses.
- **IP Address.** The IP address that the Internet (WAN) port of the router uses. If no address is shown or the address is 0.0.0.0, the router is not connected to the Internet.
- **Connection.** Shows whether the router is using a fixed or dynamic IP address on the Internet port. If the value is DHCP, the router obtains an IP address dynamically from the ISP or from a DHCP server on your LAN.
- **IP Subnet Mask.** The IP subnet mask that the Internet port of the router uses.
- **Domain Name Server.** The Domain Name Server address that the router uses. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

Statistics

The router provides various statistics.

➤ To manage the traffic statistics:

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

2. Click the **ADVANCED** tab.

The screenshot shows the web interface of the A750 Wireless Dual Band Gigabit Router JR6150. The **ADVANCED** tab is selected. The interface includes a sidebar with navigation options and a main content area with four panels:

- Router Information:** Displays hardware and firmware versions, LAN port details (MAC, IP, DHCP), and a **Reboot** button.
- Internet Port:** Displays MAC address, IP address, connection type, and subnet mask. Includes **Show Statistics** and **Connection Status** buttons.
- Wireless Settings(2.4GHz):** Displays SSID, region, channel, mode, and AP status.
- Wireless Settings(5GHz):** Displays SSID, region, channel, mode, and AP status.

3. In the Internet Port pane, click the **Show Statistics** button.

System Up Time 97:24:13

Port	Status	TxPkts	RxPkts	Collisions	Up Time
WAN	1000M/Full	11270	376786	0	97:23:10
LAN1	Link down	--	--	--	--
LAN2	Link down	--	--	--	--
LAN3	Link down	--	--	--	--
LAN4	Link down	--	--	--	--
WLAN b/g/n	300M	0	0	0	97:23:20
WLAN a/n	450M	23561	160829	0	97:23:20

Poll Interval: (secs) **Set Interval** **Stop**

The following information displays:

- **System Up Time.** The time elapsed since the router was last restarted.
 - **Port.** The statistics for the WAN (Internet) port, the four LAN (Ethernet) ports, and the wireless LAN (WLAN) port.
 - **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.
 - **Up Time.** The time elapsed since this port acquired the link.
 - **Poll Interval.** The interval at which the statistics are updated on this screen.
4. To change the polling frequency, enter a time in seconds in the **Poll Interval** field, and click the **Set Interval** button.
 5. To stop the polling entirely, click the **Stop** button.

Connection Status

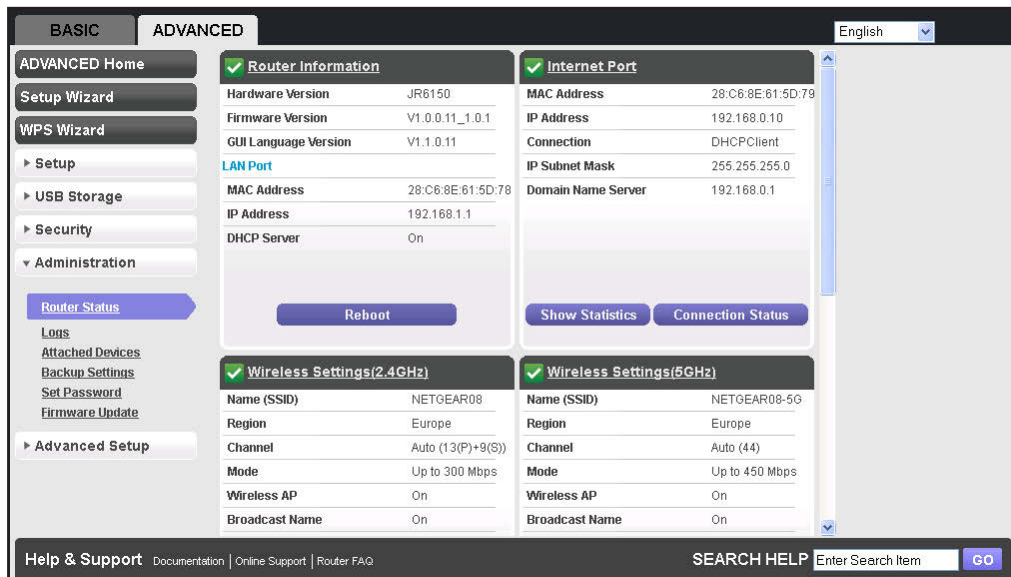
The content of this screen depends on the type of connection. For example, different information is shown for a PPPoE connection than for a DHCP connection.

➤ **To view the connection status:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Click the **ADVANCED** tab.



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



The content of the Connection Status pop-up screen depends on the type of connection. You can start new connections and end existing connections from this screen.

The following list describes the different types of connections and the associated settings that display on the Connection Status pop-up screen:

- **DHCP connection:**

The following information displays for a DHCP connection:

- **IP Address.** The IP address that is assigned to the router.
- **Subnet Mask.** The subnet mask that is assigned to the router.

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

Choose any of the following actions:

- a. To release the router's IP address and terminate the Internet connection, click the **Release** button.
- b. To let the router acquire an IP address from the DHCP server and start the Internet connection, click the **Renew** button.
- c. To close the Connection Status screen, click the **Close Window** button.

The content of the Connection Status pop-up screen depends on the type of connection.

- **PPPoE connection:**

The **Connect** and **Disconnect** buttons in the Connection Status screen display only when the connection mode is Manually Connect.

The following information displays for a PPPoE connection:

- **Connection Time.** The time that elapsed since the connection was established.
- **Connection Status.** The status of the connection: Connected, Disconnected, Negotiation (---, Success), or Authentication (---, Success). --- indicates failure.
- **IP Address.** The IP address that is assigned to the router.
- **Subnet Mask.** The subnet mask that is assigned to the router.

Choose any of the following actions:

- a. To establish the PPPoE connection manually, click the **Connect** button.
- b. To terminate the PPPoE connection manually, click the **Disconnect** button.
- c. To close the Connection Status screen, click the **Close Window** button.

The content of the Connection Status pop-up screen depends on the type of connection.

- **PPTP connection:**

The **Connect** and **Disconnect** buttons in the Connection Status screen display only when the connection mode is Manually Connect.

The following information displays for a PPTP connection:

- **Connection Status.** The status of the connection: Connected or Disconnected.
- **IP Address.** The IP address that is assigned to the router.
- **Subnet Mask.** The subnet mask that is assigned to the router.

Choose any of the following actions:

- a. To establish the PPTP connection manually, click the **Connect** button.
- b. To terminate the PPTP connection manually, click the **Disconnect** button.
- c. To close the Connection Status screen, click the **Close Window** button.

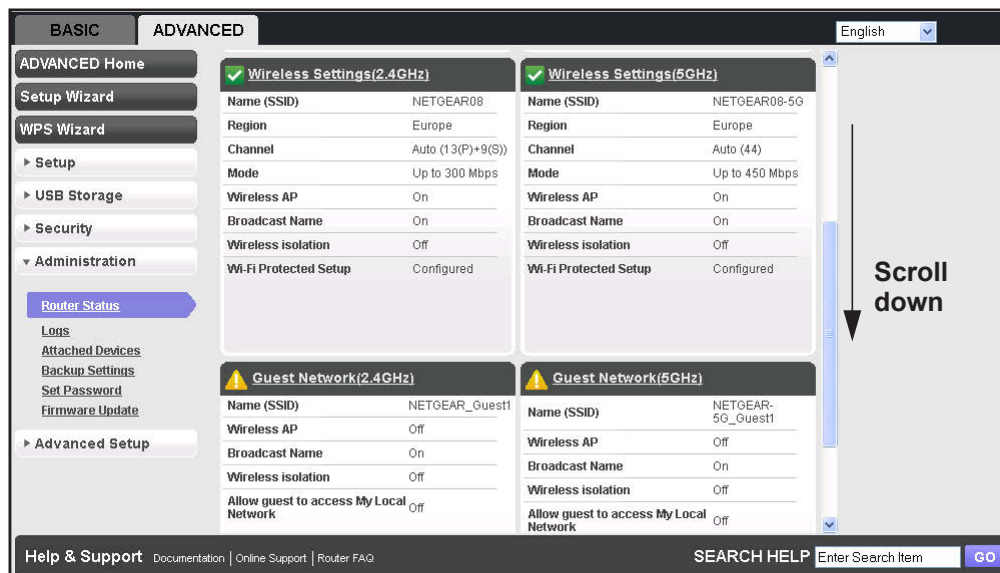
Wireless Settings Panes

➤ To display the Wireless Settings panes:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Click the **ADVANCED** tab.



Information for the 2.4 GHz and 5 GHz WiFi bands displays separately.

The following information displays:

- **Name (SSID).** The wireless network name (SSID) that the router uses.
- **Region.** The geographic region where the router is used. It might be illegal to use the wireless features of the router in some parts of the world.
- **Channel.** The operating channel of the wireless port. The default channel is Auto. When Auto is selected, the router finds the best operating channel available.
- **Mode.** The wireless communication mode: Up to 54 Mbps, Up to 150 Mbps (the default), or Up to 300 Mbps.
- **Wireless AP.** Indicates whether the radio of the router is enabled. If the radio is not enabled, the Wireless LED on the front panel is off.
- **Broadcast Name.** Indicates whether the router is broadcasting its SSID.

- **Wireless Isolation.** Indicates whether wireless isolation is on or off. When it is off, wireless clients (computers or wireless devices) that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.
- **Wi-Fi Protected Setup.** Indicates whether Wi-Fi Protected Setup is configured for this network.

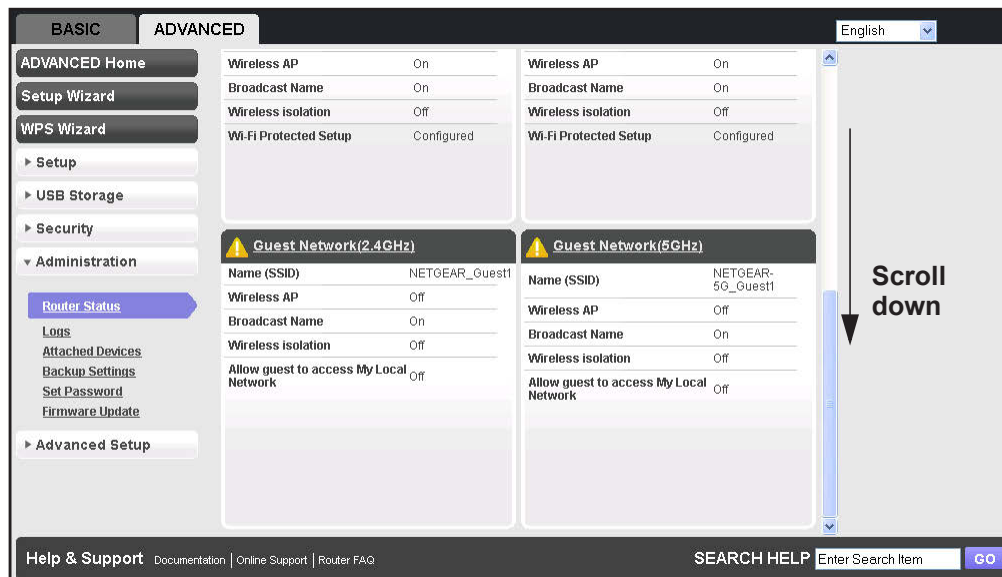
Guest Network Panes

➤ To display the Guest Network panes:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Click the **ADVANCED** tab.



Information for the 2.4 GHz and 5 GHz WiFi bands displays separately.

The following information displays:

- **Name (SSID).** The 11n wireless network name (SSID) used by the router. The default names are NETGEAR-Guest and NETGEAR-5G-Guest.
- **Wireless AP.** Indicates whether the radio feature of the router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.
- **Broadcast Name.** Indicates whether the router is broadcasting its SSID.
- **Wireless Isolation.** Prevents wireless connections to the local networks associated with the router.
- **Allow guest to access My Local Network.** Indicates whether any user who connects to this SSID can access local networks associated with the router.

View Logs of Web Access or Attempted Web Access

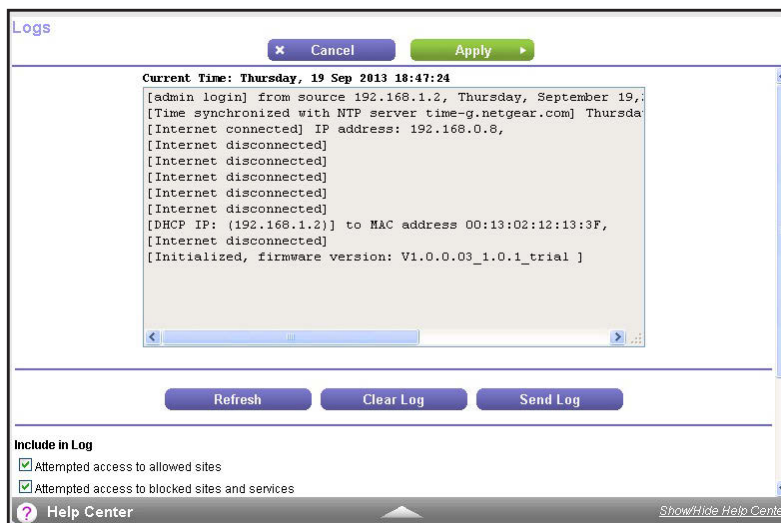
A log is a detailed record of the websites that users on your network have accessed or attempted to access. If you have set up content filtering on the Block Sites screen, the Logs screen shows you when someone on your network tried to access a blocked site. If you have email notification on, you receive these logs in an email message. If you do not have email notification set up, you can view the logs [here](#).

➤ **To view the logs:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Administration > Logs**.



The Logs screen shows the following information:

- **Source IP.** The IP address of the initiating device for this log entry.
- **Target address.** The name or IP address of the website or news group visited or to which access was attempted.
- **Action.** The action that occurred.
- **Date and time.** The date and time the log entry was recorded.

- 3.** Do any of the following:

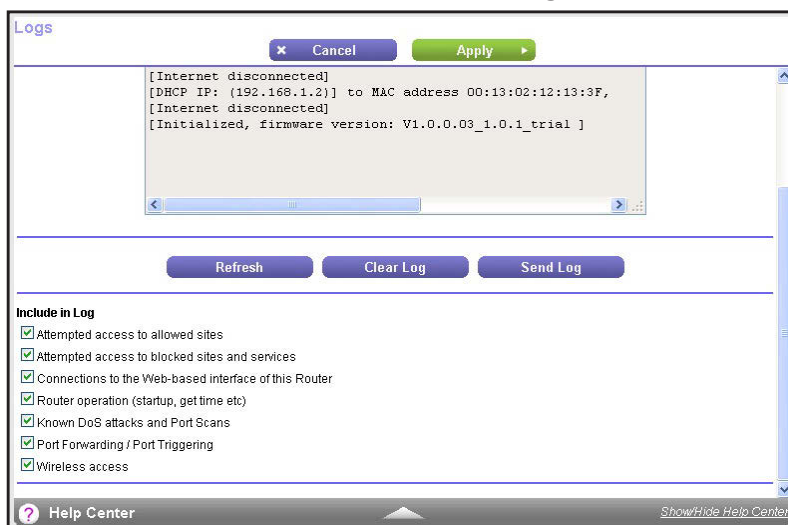
- To refresh the log screen, click the **Refresh** button.
- To clear the log entries, click the **Clear Log** button.
- To email the log, click the **Send Log** button.

➤ **To specify logs settings:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Administration > Logs**.



3. Select the following check boxes for the events that you want to include in the log:

- **Attempted access to allowed sites**
- **Attempted access to blocked sites and services**
- **Connections to the Web-based interface of this Router**
- **Router operation (startup, get time etc)**
- **Known DoS attacks and Port Scans**
- **Port Forwarding / Port Triggering**
- **Wireless access**

4. Click the **Apply** button.

Manage the Configuration File

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

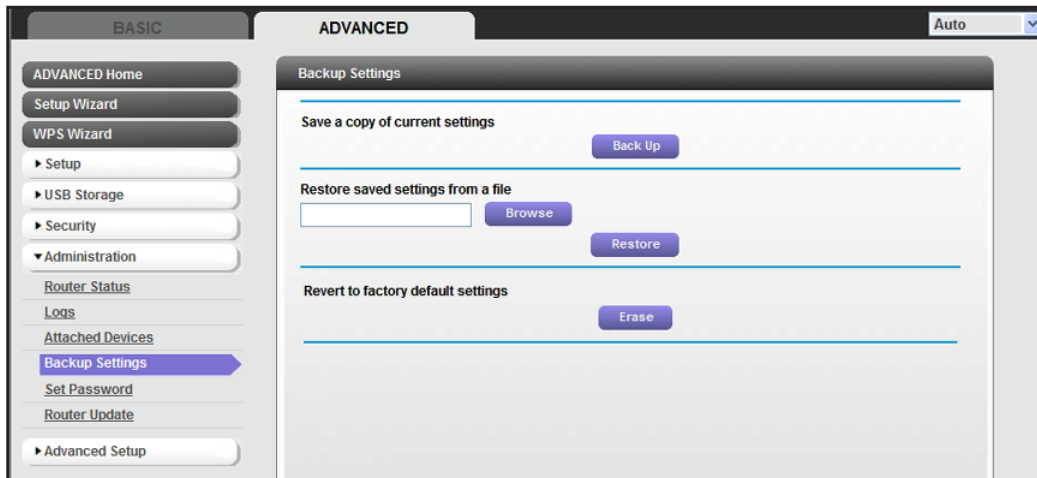
Back Up Settings

➤ **To back up the router's configuration settings:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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



3. Click the **Back Up** button.

A screen displays asking you where you want to store your settings.

4. Choose a location to store the `.cfg` file that is on a computer on your network.
5. Click the **OK** button.

A copy of the current settings is saved.

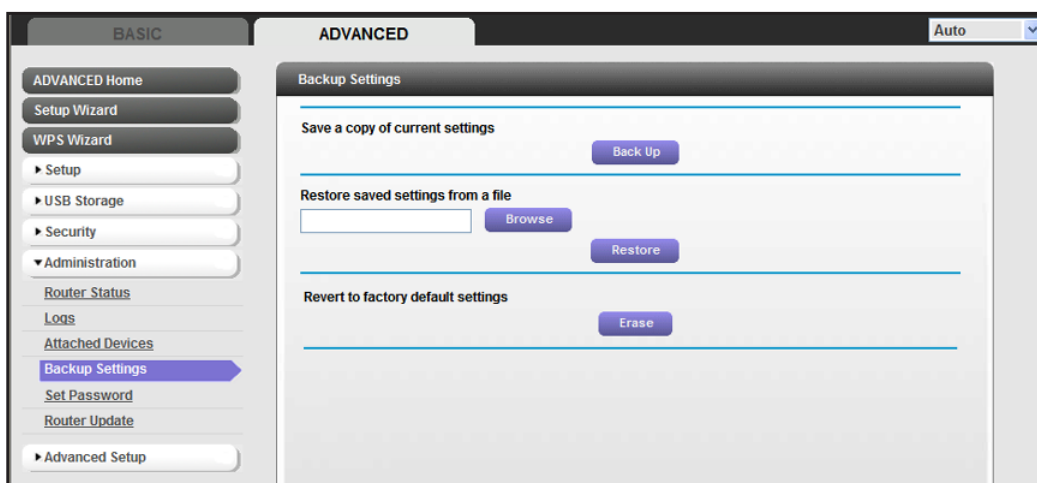
Restore Configuration Settings

- To restore configuration settings that you backed up:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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



3. Click the **Browse** button to find and select the `.cfg` file.
4. Click the **Restore** button.

The file is uploaded to the router.

The router reboots.



WARNING:

Do not interrupt the reboot process.

Erase

You can use the **Erase** button to erase the configuration and restore the factory default settings. You might want to erase the settings if you move the router to a different network.

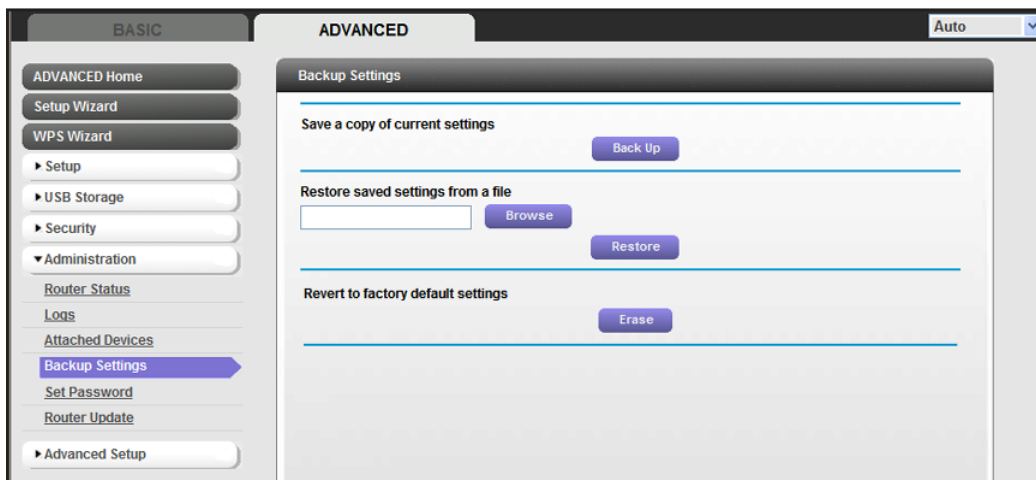
You can also use the Restore Factory Settings button of the router to erase the configuration and restore the factory settings. For more information, see *Factory Default Settings* on page 154.

➤ To erase the configuration settings:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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



3. Click the **Erase** button.

The factory default settings are restored. The password for the user name admin is password and the LAN IP address is 192.168.1.1. DHCP is enabled.

Upgrade the Router Firmware

The router firmware (routing software) is stored in flash memory. You might see a message at the top of the genie screens when new firmware is available for your product.

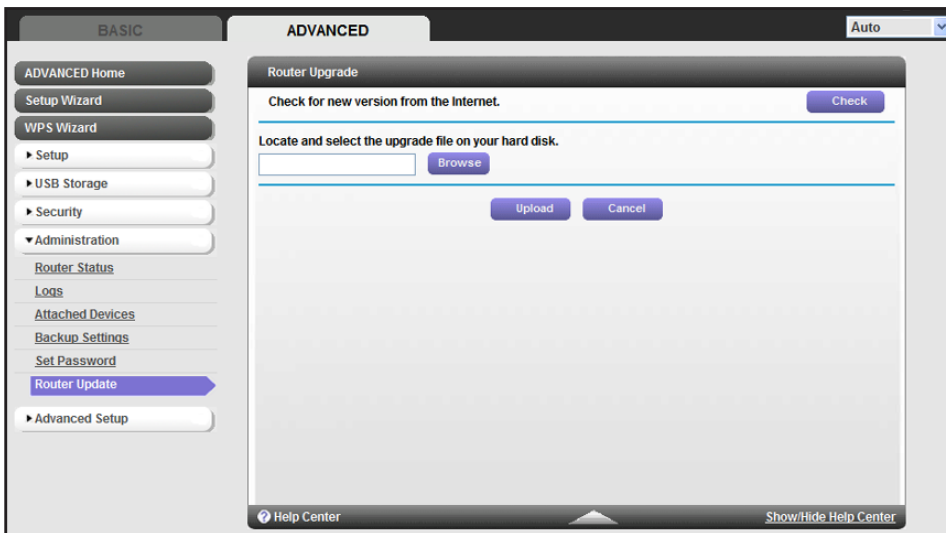
You can check and update to the latest firmware for your product when new firmware is available.

➤ **To check for new firmware and update your router:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Administration > Router Update**.

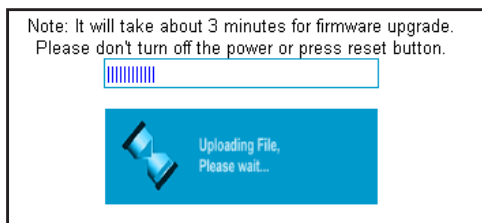


3. Click the **Check** button.

If new firmware is available, the router detects it and displays the Firmware Upgrade Assistant screen.

4. To update the router to the new firmware, click the **Yes** button.
5. If you have manually downloaded new firmware from the NETGEAR support website:
 - a. Click **Browse**, navigate to the firmware file (the file ends in `.img`), and select the firmware file.
 - b. Click the **Upload** button.

A progress bar shows the progress of the firmware upload process:





WARNING:

When uploading firmware to the router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the firmware might be corrupted.

When the upload is complete, your router restarts. The upload process can take up to three minutes, and the upgrade process typically takes about one minute. To determine whether you need to reconfigure the router after upgrading, read the new firmware release notes.

8. Advanced Settings

8

Fine-tune your network

This chapter describes the advanced features of your router. This information is for users with a solid understanding of networking concepts and who want to set up the router for unique situations such as when remote access from the Internet by IP or domain name is needed.

The chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless AP*
- *Wireless Repeating Function*
- *Port Forwarding and Port Triggering Configuration Concepts*
- *Set Up Port Forwarding to Local Servers*
- *Set Up Port Triggering*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*
- *Traffic Meter*

For added security, you can set up the router to share only approved USB devices. For more information, see *Specify Approved USB Devices* on page 74.

Advanced Wireless Settings

You can turn the wireless radio on and off, specify WPS settings, and set up a wireless access list.

The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options in this screen are reserved for wireless testing and advanced configuration only. Do not change these settings unless you have a specific reason to do so.

Control the Wireless Radio

By default, the wireless radio is enabled so that you can connect wirelessly to the router. You can turn the wireless radio on or off in the Advanced Wireless Settings screen or by using the **Wireless On/Off** button on the router front panel. When the wireless radio is off, you can still use an Ethernet cable for the WAN and LAN connections to the router.

➤ **To turn the wireless radios on or off:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

The screenshot shows the 'Advanced Wireless Settings' page. On the left is a navigation menu with options like 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup', 'USB Storage', 'Security', 'Administration', and 'Advanced Setup'. The 'Advanced Setup' section is expanded, showing 'Advanced Wireless Settings' as the selected option. The main content area has two tabs: 'BASIC' and 'ADVANCED'. The 'ADVANCED' tab is active, showing the 'Advanced Wireless Settings' page. The page has a title bar with 'Cancel' and 'Apply' buttons. The 'Wireless Network (2.4GHz b/g/n)' section has a checked 'Enable Wireless Router Radio' checkbox, followed by input fields for 'Fragmentation Length (256-2346)' (2346), 'CTS/RTS Threshold (1-2347)' (2347), and a 'Preamble Mode' dropdown (Long Preamble). Below this is a checkbox for 'Turn off wireless signal by schedule' which is unchecked. A table for scheduling is present with columns for Period, Start, End, and Recurrence Pattern. The 'Wireless Network (5GHz a/n)' section has identical settings. At the bottom, there is a 'WPS Settings' section and a 'Help Center' link.

The 2.4 GHz and 5 GHz WiFi bands are configured separately. By default, the **Enable Wireless Router Radio** check boxes are selected.

3. Select or clear the **Enable Wireless Router Radio** check box.

Clearing this check box turns off the WiFi feature of the wireless router.

4. To specify the times when you do not need a wireless connection, select the **Turn off wireless signal by schedule** check box and enter the information in the fields provided.

For example, you could turn off the wireless signal for the weekend if you leave town.

You can select the **Turn off wireless signal by schedule** check box only when **Wired WAN** mode is selected.

- Click the **Apply** button.

Your changes take effect.

Set Up a Wireless Schedule

You can use this feature to turn off the wireless signal from your router at times when you do not need a wireless connection. For example, you could turn it off for the weekend if you leave town. You can turn the wireless radio off only when the router is in Wired WAN mode.

- **To configure and enable the wireless schedule:**

- Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

The screenshot displays the 'Advanced Wireless Settings' page in the NETGEAR router's web interface. The left sidebar contains a navigation menu with options like 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup', 'USB Storage', 'Security', 'Administration', and 'Advanced Setup'. Under 'Advanced Setup', 'Advanced Wireless Settings' is highlighted. The main content area is titled 'Advanced Wireless Settings' and includes 'Cancel' and 'Apply' buttons. It is divided into two sections: 'Wireless Network (2.4GHz b/g/n)' and 'Wireless Network (5GHz a/n)'. Each section has a checked 'Enable Wireless Router Radio' checkbox, input fields for 'Fragmentation Length (256-2346)' (set to 2346) and 'CTS/RTS Threshold (1-2347)' (set to 2347), and a 'Preamble Mode' dropdown set to 'Long Preamble'. Below these, there is an unchecked checkbox for 'Turn off wireless signal by schedule'. Under this checkbox, a table is shown for scheduling the signal to turn off, with columns for 'Period', 'Start', 'End', and 'Recurrence Pattern'. Buttons for 'Add a new period', 'Edit', and 'Delete' are provided for each section. At the bottom, there is a 'WPS Settings' section and a 'Help Center' link.

The 2.4 GHz and 5 GHz WiFi bands are configured separately.

- Select the **Turn off wireless signal by schedule** check box.

The **Turn off wireless signal by schedule** check box can be selected only when the router is in Wired WAN mode.

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

- Use the lists, radio buttons, and check boxes to set up a period during which you want to turn off the wireless signal.
- Click the **Apply** button.

The Advanced Wireless Settings screen displays.

- Click the **Apply** button.

Your changes are saved.

View or Change WPS Settings

- To specify WPS settings:

- Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

The **Router's PIN** field displays the PIN that you use on a registrar (for example, from Network Explorer on a Vista Windows computer) to configure the router's wireless settings through WPS.

3. (Optional) Select or clear the **Disable Router's PIN** check box.

The PIN function might temporarily be disabled when the router detects suspicious attempts to break into the router's wireless settings by using the router's PIN through WPS. You can manually enable the PIN function by clearing the **Disable Router's PIN** check box.

4. (Optional) Select or clear the **Keep Existing Wireless Settings** check box.

The 2.4 GHz and 5 GHz WiFi bands are configured separately. By default, the **Keep Existing Wireless Settings** check boxes are selected. NETGEAR recommends that you leave this check box selected.

If you clear these check boxes, the next time a new wireless client uses WPS to connect to the router, the router wireless settings change to an automatically generated random SSID and security key.

5. Click the **Apply** button.

Your changes are saved.

Set Up a Wireless Access List by MAC Address

You can set up a list of computers and wireless devices that are allowed to join the wireless network. This list is based on the unique MAC address of each computer and device.

Each network device has a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the wireless card or network interface device. If you do not have access to the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses in the Attached Devices screen.

➤ To restrict access based on MAC addresses:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

The screenshot shows the 'Advanced Wireless Settings' page. The left sidebar contains navigation links: ADVANCED Home, Setup Wizard, WPS Wizard, Setup, USB Storage, Security, Administration, and Advanced Setup. Under Advanced Setup, 'Advanced Wireless Settings' is selected. The main content area includes sections for 'Wireless Network (5GHz a/n)', 'Turn off wireless signal by schedule', 'WPS Settings', and 'Wireless Card Access List'. The 'Wireless Card Access List' section has a 'Set Up Access List' button. A vertical arrow on the right side of the page points downwards with the text 'Scroll down'.

3. Scroll down and click the **Set Up Access List** button.

The screenshot shows the 'Wireless Card Access List' screen. It features a table with two columns: 'Device Name' and 'MAC Address'. Below the table are buttons for '+ Add', 'Edit', and 'Delete'. Above the table is a checkbox labeled 'Turn Access Control On'. At the top of the screen are 'Cancel' and 'Apply' buttons.

4. On the Wireless Card Access List screen, click the **Add** button.

The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

The screenshot shows the 'Wireless Card Access Setup' screen. It features a table with three columns: '#', 'Device Name', and 'MAC Address'. Below the table are input fields for 'Device Name' and 'MAC Address'. At the top of the screen are 'Refresh', 'Cancel', and 'Add' buttons.

5. If the computer or device you want is in the Available Wireless Cards list, select that radio button; otherwise, type a name and the MAC address.

You can usually find the MAC address on the label of the wireless device.

Tip: You can copy and paste the MAC addresses from the Attached Devices screen into the MAC Address field of this screen. Take this action to have each wireless computer join the wireless network. The computer then displays in the Attached Devices screen.

For more information about the attached devices, see [Attached Devices](#) on page 32.

6. Click the **Add** button.

The screen changes back to the list screen.

7. Add each computer or device that you want to allow to connect wirelessly.
8. Select the **Turn Access Control On** check box.
9. Click the **Apply** button.

➤ **To edit a wireless device or delete it from the access list:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

The Advanced Wireless Settings screen displays.

3. In the table, select the radio button next to the wireless device that you want to edit or delete.

4. Do one of the following:

- Click the **Edit** button.

The Edit Wireless Card screen displays.

- a. Edit the address information.

- b. Click the **Accept** button.

- Click the **Delete** button.

The address is removed from the table.

Wireless AP

The router can function in access point (AP) mode instead of regular router mode. In AP mode, the router can function as a bridge between wireless clients and another router or gateway in your network that connects to the Internet. When the router functions in AP mode, many router functions are disabled, but wireless clients can connect to the router. You can still access the router to change the configuration, for example, to disable AP mode and return to regular router mode.

➤ **To enable and configure AP mode:**

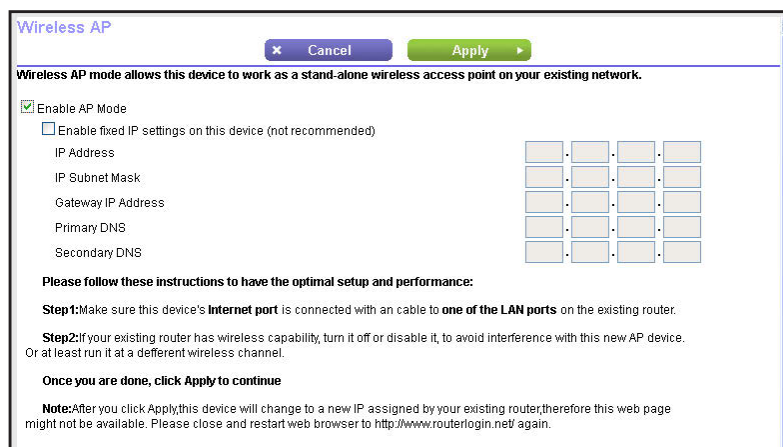
1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Advanced Setup > Wireless AP.**



3. Select the **Enable Access Point Mode** check box.



4. (Optional) Select the **Enable fixed IP settings on this device** check box.

NETGEAR recommends that you do not use this feature.

5. Enter the following information about your Internet connection:

- **IP Address.** The IP address that your ISP assigned.
- **IP Subnet Mask.** The IP subnet mask that your ISP assigned.
- **Gateway IP Address.** The gateway IP address that your ISP assigned. The gateway is the ISP's router to which your router connects.
- **Primary DNS.** The IP address of your ISP's primary DNS server.
- **Secondary DNS.** The IP address of your ISP's secondary DNS server.

6. Click the **Apply** button.

Your settings are saved.

7. If you lose this screen, close and restart web browser.

The router changes to a new IP address that is assigned by your existing router. As a result, this screen might not display.

8. Enter **www.routerlogin.net** and log in again.

Wireless Repeating Function

You can set up the router to be used as a wireless base station or wireless repeater in a wireless distribution system (WDS). A WDS lets you expand a wireless network through multiple access points instead of using a wired backbone to link them. A wireless base station connects to the Internet, can have wired and wireless clients, and sends its wireless signal to an access point that functions as a wireless repeater. A wireless repeater can also have wired and wireless clients, but connects to the Internet through the wireless base station.

The following figure shows a wireless repeating scenario.

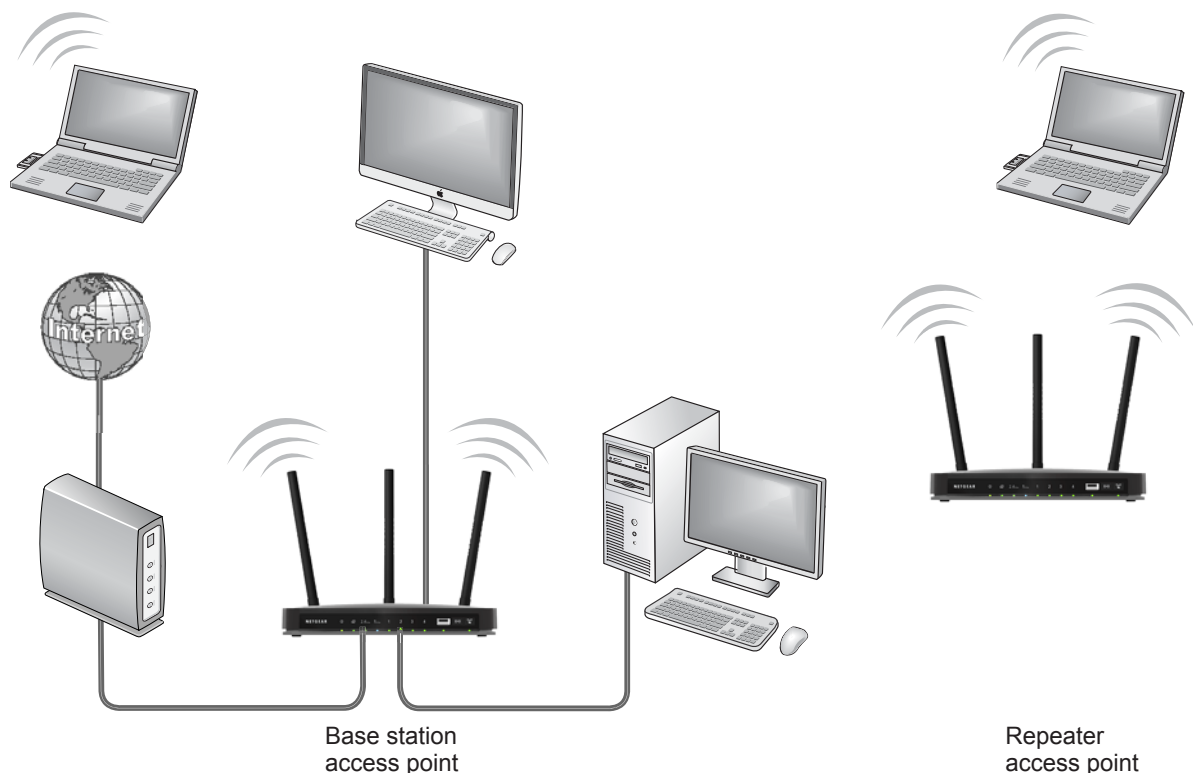


Figure 8. Wireless repeating scenario

The router can function either as a base station or as a repeater:

- **Wireless base station.** The router acts as the parent access point, bridging traffic to and from the child repeater access point, as well as handling wireless and wired local computers. To configure this mode, you must know the MAC addresses of the child repeater access point.

- **Wireless repeater.** The router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you must know the MAC address of the remote parent access point.

For you to set up a wireless network in a WDS, the following conditions must be met for both access points:

- Both access points must use the same SSID, wireless channel, and encryption mode.
- Both access points must be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) must be configured to operate in the same LAN network address range as the access points.
- The channel selection on the access points cannot be **Auto** (see [Basic Wireless Settings](#) on page 25).
- The security option must be WEP (or no security). The **WEP** option displays only if you select **Up to 54 Mbps** from the **Mode** list on the Wireless Settings screen (see [Basic Wireless Settings](#) on page 25).

Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You must know the wireless MAC addresses of all units. First, set up the base station and then set up the repeater.

➤ To set up the base station:

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

2. Select **ADVANCED > Advanced Setup > Wireless Repeating Function**.

The screenshot displays the 'Wireless Repeating Function' configuration page in the router's web interface. The 'ADVANCED' tab is selected, and the 'Wireless Repeating Function' sub-tab is active. The page is divided into two main sections: '2.4GHz b/g/n' and '5GHz a/n'. In the 2.4GHz section, the 'Enable Wireless Repeating Function' checkbox is checked. Below it, there are options to 'Disable Wireless Client Association' and a field for 'Wireless MAC of this router' showing '28:C6:8E:61:5D:78'. The 'Wireless Repeater' radio button is selected, showing a 'Repeater IP Address' of '192.168.1' and a 'Base Station MAC Address' field. The 'Wireless Base Station' radio button is unselected, showing four 'Repeater MAC Address' fields. The 5GHz section is disabled, with the 'Enable Wireless Repeating Function' checkbox unchecked. The left sidebar contains a navigation menu with options like 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup', 'USB Storage', 'Security', 'Administration', 'Advanced Setup' (selected), 'Advanced Wireless Settings', 'Wireless AP', 'Wireless Repeating Function' (highlighted), 'Port Forwarding / Port Triggering', 'Dynamic DNS', 'Static Routes', 'Remote Management', 'USB Settings', 'UPnP', and 'Traffic Meter'. The bottom of the page features a 'Help Center' link and a 'Show/Hide Help Center' button.

The wireless MAC address of the router displays onscreen. The 2.4 GHz and 5 GHz WiFi bands are configured separately.

3. Select the **Enable Wireless Repeating Function** check box.
4. Select the **Wireless Base Station** radio button.

5. To prevent wireless clients from associating with the base station and allow LAN client associations only, select the **Disable Wireless Client Association** check box.

You can leave the check box cleared if you prefer wireless clients to be able to associate with the base stations.

6. In the **Repeater MAC Address 1** through **4** fields, enter the MAC addresses for the access points that will function as repeaters.

If your router is the base station, it can function as the “parent” for up to four other access points.

7. Click the **Apply** button.

Set Up a Repeater

To set up the repeater to avoid conflicts with the wireless connection to the base station, use a wired Ethernet connection.

Note: If you set up your router as a base station with a non-NETGEAR access point as the repeater, you might need to change more configuration settings. In particular, you should disable the DHCP server function on the access point that functions as the repeater.

➤ To configure the router as a repeater:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Advanced Setup > Wireless Repeating Function**.

The screenshot shows the 'Wireless Repeating Function' configuration page. The left sidebar contains a navigation menu with 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup', 'USB Storage', 'Security', 'Administration', and 'Advanced Setup'. Under 'Advanced Setup', there are links for 'Advanced Wireless Settings', 'Wireless AP', 'Wireless Repeating Function' (highlighted), 'Port Forwarding / Port Triggering', 'Dynamic DNS', 'Static Routes', 'Remote Management', 'USB Settings', 'UPnP', and 'Traffic Meter'. The main content area has tabs for 'BASIC' and 'ADVANCED'. The 'ADVANCED' tab is active, showing the 'Wireless Repeating Function' settings. There are two sections: one for 2.4GHz and one for 5GHz. In both sections, the 'Enable Wireless Repeating Function' checkbox is unchecked. The 'Wireless Repeater' radio button is selected in both sections. The 'Repeater IP Address' field is set to 192.168.1.1 in both sections. The 'Base Station MAC Address' field is empty in both sections. The 'Wireless Base Station' radio button is unselected in both sections. The 'Repeater MAC Address 1' through 'Repeater MAC Address 4' fields are empty in both sections. The 'Wireless MAC of this router' is displayed as 28:C6:8E:61:5D:78 for both sections. There are 'Cancel' and 'Apply' buttons at the top right of the 2.4GHz section.

The wireless MAC address of the router displays onscreen. The 2.4 GHz and 5 GHz WiFi bands are configured separately.

3. Select the **Enable Wireless Repeating Function** check box.
4. Select the **Wireless Repeater** radio button.

This screenshot is identical to the previous one, but the 'Enable Wireless Repeating Function (2.4GHz b/g/n)' checkbox is now checked. The 'Wireless Repeater' radio button remains selected. The 'Repeater IP Address' field is still 192.168.1.1. The 'Base Station MAC Address' field is still empty. The 'Wireless Base Station' radio button is still unselected. The 'Enable Wireless Repeating Function (5GHz a/n)' checkbox is still unchecked. The 'Wireless Repeater' radio button is still selected. The 'Repeater IP Address' field is still 192.168.1.1. The 'Base Station MAC Address' field is still empty. The 'Wireless MAC of this router' is still 28:C6:8E:61:5D:78 for both sections. The 'Cancel' and 'Apply' buttons are still present at the top right of the 2.4GHz section.

5. Complete the **Repeater IP Address** field.

This IP address must be in the same subnet as the base station, but different from the LAN IP address of the base station.

6. To prevent wireless clients from associating with the repeater and allow LAN client associations only, select the **Disable Wireless Client Association** check box.

You can leave the check box cleared if you prefer wireless clients to be able to associate with the repeater.

7. In the **Base Station MAC Address** field, enter the MAC address for the access point that functions as the base station.
8. Click the **Apply** button.
9. Verify connectivity across the LANs.

A computer on any wireless or wired LAN segment of the base station or a repeater can connect to the Internet. Any computer that is connected to the base station can share files and printers with any other wireless or wired computer or server that is connected to a repeater.

Port Forwarding and Port Triggering Configuration Concepts

By default, the router blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You might need to create exceptions to this rule for these purposes:

- To allow remote computers on the Internet to access a server on your local network
- To allow certain applications and games to work correctly when your router does not recognize their replies

Your router provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your router must modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type `http://www.example.com` into the URL field, and your computer creates a web page request message and sends it to your router. The message contains the following address and port information:
 - **Source address.** Your computer's IP address.
 - **Source port number.** 5678, which is the browser session.

- **Destination address.** The IP address of www.example.com, which your computer finds by asking a DNS server.
 - **Destination port number.** 80, which is the standard port number for a web server process.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at www.example.com. Before sending the web page request message to www.example.com, your router stores the original information and then performs Network Address Translation (NAT) and modifies the following source information in the request message:
- The source address is replaced with your router's public IP address. This replacement is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
 - The source port number is changed to a number chosen by the router, such as 33333. This change is necessary because two computers could independently be using the same session number.

Your router then sends this request message through the Internet to the web server at www.example.com.

4. The web server at www.example.com composes a return message with the requested web page data. The web server then sends this reply message to your router. The return message contains the following address and port information:
- **Source address.** The IP address of www.example.com.
 - **Source port number.** 80, which is the standard port number for a web server process.
 - **Destination address.** The public IP address of your router.
 - **Destination port number.** 33333.
5. When your router receives the incoming message, it checks its session table for an active session for port number 33333. Finding an active session, the router then modifies the message to restore the original address information replaced by NAT. Your router sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information:
- **Source address.** The IP address of www.example.com.
 - **Source port number.** 80, which is the standard port number for a web server process.
 - **Destination address.** Your computer's IP address.
 - **Destination port number.** 5678, which is the browser session that made the initial request.
6. When you finish your browser session, your router eventually detects a period of inactivity in the communications. Your router then removes the session information from its session table, and port number 33333 no longer accepts incoming traffic.

Port Triggering to Open Incoming Ports

In the preceding example, your router sends requests to a remote computer from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply to a different port number, your router does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies to multiple port numbers. Using the port triggering function of your router, you can tell the router to open more incoming ports when a particular outgoing port originates a session.

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

Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, say port 33333) as the destination port. The IRC server also sends an “identify” message to your router with destination port 113.
6. When your router receives the incoming message to destination port 33333, it checks its session table for an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. When your router receives the incoming message to destination port 113, it checks its session table and finds an active session for port 113 associated with your computer. The router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you must know which inbound ports the application needs. Also, you must know the number of the outbound port that triggers the opening of the inbound ports. You can usually find this information by contacting the publisher of the application or user groups or newsgroups.

Note: Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser must access a web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:
 - **Destination address.** The IP address of www.example.com, which is the address of your router.
 - **Destination port number.** 80, which is the standard port number for a web server process.

The remote computer then sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message.

The destination address is replaced with 192.168.1.123.

Your router then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your router.
4. Your router performs Network Address Translation (NAT) on the source IP address and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you must know which inbound ports the application needs. You can usually find this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Any computer on your network can use port triggering, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- Port triggering does not require that you know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Set Up Port Forwarding to Local Servers

You can configure the router to forward specific incoming protocols to computers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded. Before starting, you must determine which type of service, application, or game you want to provide, and the local IP address of the computer that should provide the service. The server computer must always have the same IP address.

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature (see [Address Reservation](#) on page 50) of your router.

➤ To set up port forwarding:

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

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

The screenshot shows the 'Port Forwarding / Port Triggering' configuration page. The left sidebar has a menu with 'Port Forwarding / Port Triggering' highlighted. The main content area has a 'Service Name' dropdown set to 'FTP'. Below it, the 'Internal IP address' is '192.168.1' with an 'Add' button. A table with the following columns is shown: #, Service Name, External Starting Port, External Ending Port, Internal Starting Port, Internal Ending Port, and Internal IP address. At the bottom of the table are buttons for 'Edit Service', 'Delete Service', and 'Add Custom Service'.

By default, **Port Forwarding** is selected as the service type.

3. From the **Service Name** list, select the service or game that you are hosting on your network.

If the service does not display in the list, see [Add a Custom Service](#) on page 123.

4. In the corresponding **Server IP Address** field, enter the last octet of the IP address of your local computer that provides this service.

5. Click the **Add** button.

The service is added to the table onscreen.

Add a Custom Service

To define a service, game, or application that does not display in the **Service Name** list, you must first find out which port number or range of numbers the application uses. You can usually find this information by contacting the publisher of the application or user groups or newsgroups.

➤ **To add a custom service:**

1. Log in to the router.

For more information, see [Use NETGEAR genie after Installation](#) on page 17.

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

Port Forwarding / Port Triggering

Please select the service type.

☒ Port Forwarding
☐ Port Triggering

Service Name: FTP Internal IP address: 192.168.1

#	Service Name	External Starting Port	External Ending Port	Internal Starting Port	Internal Ending Port	Internal IP address

Buttons: Edit Service, Delete Service, Add Custom Service

By default, **Port Forwarding** is selected as the service type.

3. Click the **Add Custom Service** button.

Ports - Custom Services

Buttons: Cancel, Apply

Service Name: [Empty]

Service Type: TCP/UDP

External Starting Port: (1~65534)

External Ending Port: (1~65534)

☐ Use the same port range for internal port

Internal Starting Port: (1~65534)

Internal Ending Port: (1~65534)

Internal IP address: 192.168.1

Or select from currently attached devices

	IP Address	Device Name
☐	192.168.1.2	MPAWLAN-SPARE

4. In the **Service Name** field, enter a descriptive name.
5. In the **Service Type** list, select the protocol. Select **TCP**, **UDP**, or **TCP/UDP**.
If you are not sure, select **TCP/UDP**.
6. In the **External Starting Port** field, enter the beginning port number.
7. In the **External Ending Port** field, enter one of the following:
 - If the application uses a single port, enter the same port number in the **External Ending Port** field.

- If the application uses a range of ports, enter the ending port number of the range in the **External Ending Port** field.

If the internal port numbers are the same as the external port numbers, select the **Use the same port range for Internal port** check box. If they are not, complete the **Internal Starting Port** and **Internal Ending Port** fields.

8. In the **Internal IP Address** field, enter the IP address of your local computer that provides this service.

You can also select a radio button for one of the devices in the list of attached devices to automatically place the IP address of the selected device in the **Internal IP Address** field.

9. Click the **Apply** button.

The service is added to the table on the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

- To edit or delete a port forwarding entry:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

The screenshot shows the 'Port Forwarding / Port Triggering' configuration page. The sidebar on the left includes options like 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', and 'Advanced Setup'. The main area has a 'Please select the service type.' section with 'Port Forwarding' selected. Below this, there are input fields for 'Service Name' (FTP), 'Internal IP address' (192.168.1), and a table with columns for Service Name, External Starting Port, External Ending Port, Internal Starting Port, Internal Ending Port, and Internal IP address. At the bottom of the table are buttons for 'Edit Service', 'Delete Service', and 'Add Custom Service'.

By default, **Port Forwarding** is selected as the service type.

3. In the table, select the radio button next to the service that you want to edit or delete.

- a. To edit the service, click the **Edit Service** button.

The screenshot shows the 'Ports - Custom Services' configuration page in the router's web interface. The 'ADVANCED' tab is selected. The left sidebar contains a menu with 'Advanced Setup' expanded, showing options like 'Port Forwarding / Port Triggering', 'Dynamic DNS', 'Static Routes', 'Remote Management', 'USB Settings', 'UPnP', and 'Traffic Meter'. The main content area has a table for configuring services. The table has columns for Service Name, Service Type, External Starting Port, External Ending Port, Internal Starting Port, Internal Ending Port, and Internal IP address. A checkbox 'Use the same port range for internal port' is checked. Below the table is a section 'Or select from currently attached devices' with a table showing IP Address and Device Name. The first entry is 192.168.1.2 for MP/WLAN-SPARE. Buttons for Cancel and Apply are at the top right of the table area.

- a. Edit the service.
b. Click the **Apply** button.
- b. To delete the service, click the **Delete Service** button.

The service is removed from the table.

Application Example: Make a Local Web Server Public

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

➤ To make a local web server public:

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation.

In this example, your router always gives your web server an IP address of 192.168.1.33. For more information, see [Address Reservation](#) on page 50.

2. On the Port Forwarding/Port Triggering screen, configure the router to forward the HTTP service to the local address of your web server at 192.168.1.33.

HTTP (port 80) is the standard protocol for web servers. For more information, see [Set Up Port Forwarding to Local Servers](#) on page 122.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name.

To access your web server from the Internet, a remote user must know the IP address that your ISP has assigned. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org. For more information, see [Dynamic DNS](#) on page 131.

Set Up Port Triggering

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

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application must open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound trigger port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

Port forwarding creates a static mapping of a port number or range to a single local computer. Port triggering can dynamically open ports to any computer that needs them and can 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 *Universal Plug and Play* on page 138.

To set up port triggering, you must know which inbound ports the application needs. Also, you must know the number of the outbound port that triggers the opening of the inbound ports. You can usually find this information by contacting the publisher of the application or user groups or newsgroups.

➤ **To set up port triggering:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

Port Forwarding / Port Triggering

Please select the service type.

☒ Port Forwarding
☐ Port Triggering

Service Name: FTP Internal IP address: 192.168.1.1

#	Service Name	External Starting Port	External Ending Port	Internal Starting Port	Internal Ending Port	Internal IP address
Edit Service Delete Service Add Custom Service						

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

Port Forwarding / Port Triggering

☐ Port Forwarding
☒ Port Triggering

☐ Disable Port Triggering

Port Triggering Time-out (in minutes): 20

#	Enable	Service Name(If Required)	Service Type	Inbound Connection	Service User
Add Service Edit Service Delete Service					

4. Clear the **Disable Port Triggering** check box if it is selected.

Note: If the **Disable Port Triggering** check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.

5. In the **Port Triggering Time-out** field, enter a value up to 9999 minutes.

The default value is 20 minutes. This value controls the inactivity timer for the designated inbound ports. Because the router cannot detect when the application has terminated, the

inbound ports close when the inactivity time expires.

6. Click the **Add Service** button.

The screenshot shows the 'Port Triggering Rule' configuration page. The interface has a sidebar on the left with a tree view containing: ADVANCED Home, Setup Wizard, WPS Wizard, Setup, USB Storage, Security, Administration, Advanced Setup, Advanced Wireless Settings, Wireless AP, Wireless Repeating Function, Port Forwarding / Port Triggering (highlighted), Dynamic DNS, Static Routes, Remote Management, USB Settings, UPnP, and Traffic Meter. The main content area is titled 'Port Triggering Rule' and has 'Cancel' and 'Apply' buttons at the top. It is divided into two sections: 'Service' and 'Required Inbound Connection'. The 'Service' section includes fields for 'Service Name (If Required):', 'Service User:' (a dropdown menu currently showing 'Any'), 'Service Type:' (a dropdown menu currently showing 'TCP'), and 'Triggering Port:' (a text input field with a range '(1~65535)' to its right). The 'Required Inbound Connection' section includes 'Service Type:' (a dropdown menu currently showing 'TCP'), 'Starting Port:' (a text input field with a range '(1~65535)' to its right), and 'Ending Port:' (a text input field with a range '(1~65535)' to its right). At the bottom of the sidebar, there is a 'Help Center' link and a 'Show/Hide Help Center' button.

7. In the **Service Name** field, type a descriptive service name.
8. In the **Service User** list, select **Any** (the default) to allow any computer on the Internet to use this service.

Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.
9. In the **Service Type** list, select the protocol. Select either **TCP** or **UDP** or **TCP/UDP**.
10. In the **Triggering Port** field, enter the number of the outbound traffic port that should open the inbound ports.
11. Enter the inbound connection port information in the **Connection Type**, **Starting Port**, and **Ending Port** fields.
12. Click the **Apply** button.

The service is added to the Port Triggering Portmap Table on the Port Forwarding/Port Triggering screen. By default, the service is enabled, that is, the **Enable** check box is selected.

➤ **To edit or delete a port triggering entry:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

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

4. In the Port Triggering Portmap Table, select the radio button next to the service that you want to edit or delete.

- a. To edit the service, click the **Edit Service** button.

- a. Edit the service.
 b. Click the **Apply** button.
- b. To delete the service, click the **Delete Service** button.
 The service is removed from the table.

Dynamic DNS

If your Internet service provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address is, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

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 router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at <http://www.dyndns.org> and obtain an account and host name that you configure in the router. Then, whenever your ISP-assigned IP address changes, your router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at <http://hostname.dyndns.org>.

Note: Before you set up Dynamic DNS on router, first register an account with one of the Dynamic DNS service providers whose URLs display in the **Service Provider** list on the Dynamic DNS screen.

➤ **To set up Dynamic DNS:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Advanced Setup > Dynamic DNS**.

3. Select the **Use a Dynamic DNS Service** check box.
4. Select the URL of your Dynamic DNS service provider.
5. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
6. Type the user name for your Dynamic DNS account.
This name is the name that you use to log in to your account, not your host name.
7. Type the password (or key) for your Dynamic DNS account.
8. Click the **Apply** button.
9. To verify the Dynamic DNS status, click the **Show Status** button.

Static Routes

Static routes provide more routing information to your router. Under usual circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure more static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets on your network.

As an example of when a static route is needed, consider a situation with the following elements:

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

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

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. This example assumes the following settings:

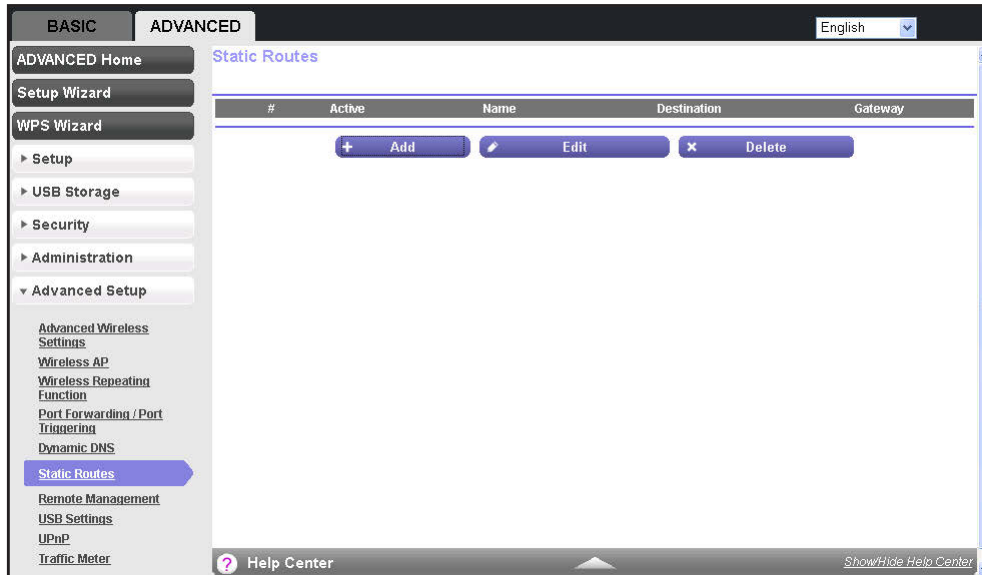
- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** field specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.1.100.
- A metric value of **1** works because the ISDN router is on the LAN.
- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

➤ **To set up a static route:**

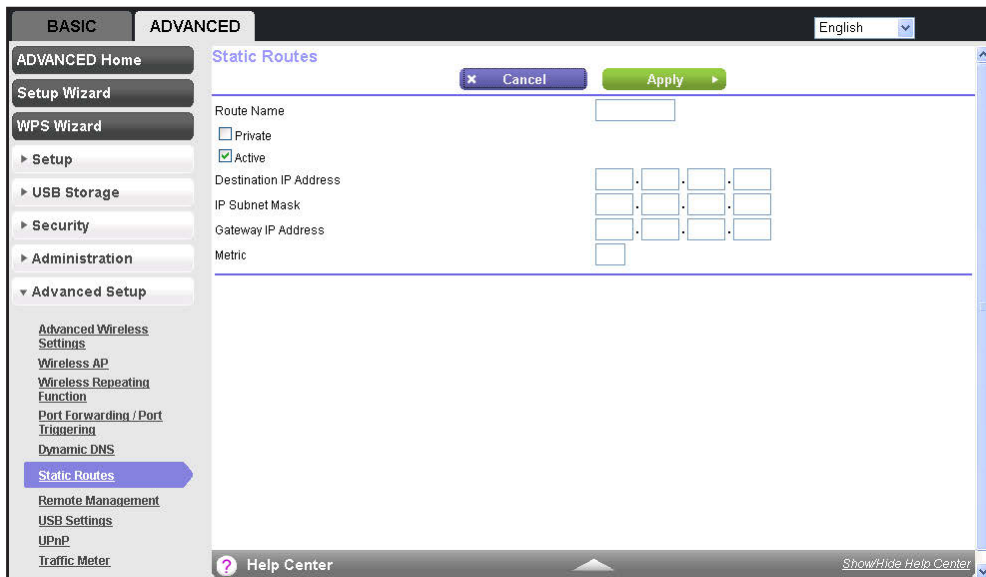
1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED** > **Advanced Setup** > **Static Routes**.



3. Click the **Add** button.



4. In the **Route Name** field, type a name for this static route (for identification purposes only.)
5. If you want to limit access to the LAN only, select the **Private** check box.
If you select **Private**, the static route is not reported in RIP.
6. To make this route effective, select the **Active** check box.
By default, the **Active** check box is selected.
7. Type the IP address of the final destination.
8. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.

9. Type the gateway IP address, which must be a router on the same LAN segment as the A750 Wireless Dual Band Gigabit Router.

10. Type a number from 1 through 15 as the metric value.

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

11. Click the **Apply** button.

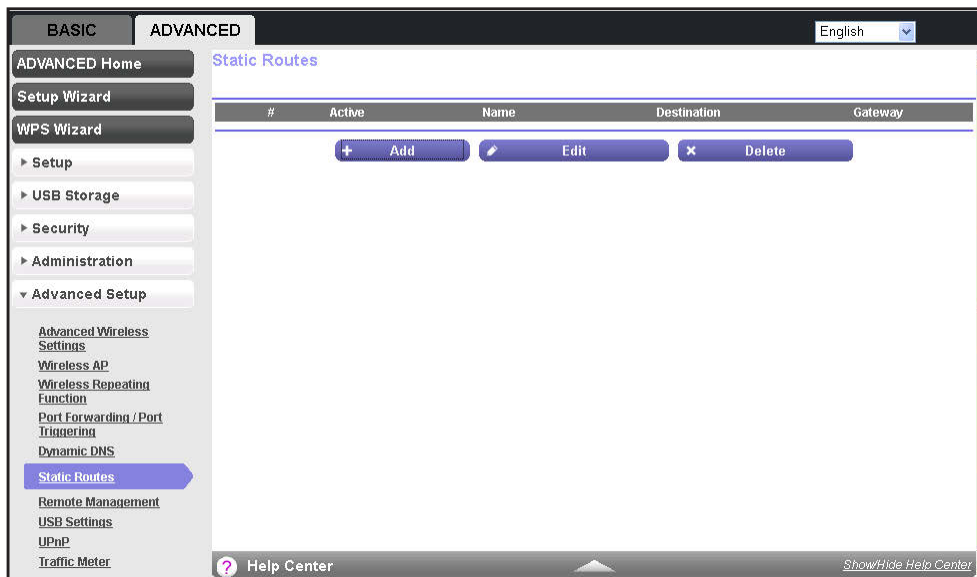
The route is added to the table on the Static Routes screen.

➤ **To edit or delete a static route:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Advanced Setup > Static Routes**.



3. In the table, select the radio button next to the route that you want to edit or delete.

- a. To edit the route, click the **Edit** button.

The screenshot shows the 'Static Routes' configuration page. The sidebar on the left includes links for 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup', 'USB Storage', 'Security', 'Administration', 'Advanced Setup', 'Advanced Wireless Settings', 'Wireless AP', 'Wireless Repeating Function', 'Port Forwarding / Port Triggering', 'Dynamic DNS', 'Static Routes' (highlighted), 'Remote Management', 'USB Settings', 'UPnP', and 'Traffic Meter'. The main content area is titled 'Static Routes' and contains a 'Cancel' button and an 'Apply' button. Below these are input fields for 'Route Name', 'Private' (checkbox), 'Active' (checkbox), 'Destination IP Address', 'IP Subnet Mask', 'Gateway IP Address', and 'Metric'. The 'Route Name' field is empty. The 'Private' checkbox is unchecked. The 'Active' checkbox is checked. The 'Destination IP Address' field is empty. The 'IP Subnet Mask' field is empty. The 'Gateway IP Address' field is empty. The 'Metric' field is empty.

- a. Edit the route information.
b. Click the **Apply** button.
- b. To delete the route, click the **Delete** button.

The route is removed from the table.

Remote Management

You can upgrade or check the status of your router over the Internet.

Note: Before you enable remote management, be sure to change the router's default login password to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

➤ **To set up remote management:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Advanced Setup > Remote Management**.

The screenshot shows the 'Remote Management' configuration page in the router's web interface. The sidebar on the left includes options like 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', 'Setup', 'USB Storage', 'Security', 'Administration', and 'Advanced Setup'. Under 'Advanced Setup', there are links for 'Advanced Wireless Settings', 'Wireless AP', 'Wireless Repeating Function', 'Port Forwarding / Port Triggering', 'Dynamic DNS', 'Static Routes', 'Remote Management' (which is highlighted), 'USB Settings', 'UPnP', and 'Traffic Meter'. The main content area has a title bar with 'Remote Management' and 'Cancel'/'Apply' buttons. Below this is a checkbox for 'Turn Remote Management On'. The 'Remote Management Address' field is populated with 'https://192.168.0.10:8443'. Under 'Allow Remote Access By', the 'Everyone' radio button is selected. The 'Port Number' field is set to '8443'. At the bottom, there is a 'Help Center' link.

3. Select the **Turn Remote Management On** check box.
4. Under Allow Remote Access By, specify the external IP addresses that the router's remote management allows.

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

Select one of the following radio buttons:

- To allow access from a single IP address on the Internet, select the **Only This Computer** radio button. Enter the IP address that is allowed access.
- To allow access from a range of IP addresses on the Internet, select the **IP Address Range** radio button. To define the allowed range, enter a beginning and ending IP address.
- To allow access from any IP address on the Internet, select the **Everyone** radio button.

5. Specify the port number for accessing the router user interface.

Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote router user interface. Choose a number from 1024 through 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

6. Click the **Apply** button.

When you access your router from the Internet, type your router's 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 8080, enter **http://203.0.113.123:8080** in your browser.

Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances 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.

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

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

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Advanced Setup > UPnP**.

The screenshot shows the 'UPnP' configuration page in the router's web interface. The left sidebar lists various settings, with 'UPnP' selected. The main area has tabs for 'BASIC' and 'ADVANCED', with 'ADVANCED' selected. The 'UPnP' section includes a 'Turn UPnP On' checkbox (checked), an 'Advertisement Period (in minutes)' field (30), and an 'Advertisement Time to Live (in hops)' field (4). Below these is a table titled 'UPnP Portmap Table' with columns: Active, Protocol, Int. Port, Ext. Port, and IP Address. The table is currently empty. At the bottom, there are buttons for 'Refresh', 'Cancel', and 'Apply'.

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

This check box is selected by default. You can enable or disable UPnP for automatic device configuration. If the **Turn UPnP On** check box is cleared, the router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.

4. Type the advertisement period in minutes.

The advertisement period specifies how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of more

network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

5. Type the advertisement time to live in hops.

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

6. Click the **Apply** button.

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

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

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic passing through your router's 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.

➤ To start monitoring Internet traffic:

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

The screenshot shows the 'Traffic Meter' configuration page in the router's web interface. The left sidebar contains a navigation menu with 'ADVANCED Home', 'Setup Wizard', 'WPS Wizard', and 'Advanced Setup' expanded. Under 'Advanced Setup', 'Traffic Meter' is selected. The main content area has a 'Traffic Meter' title bar with 'Cancel' and 'Apply' buttons. Below this, the 'Internet Traffic Meter' section has a checkbox for 'Enable Traffic Meter'. If enabled, there are three radio button options for 'Traffic volume control by': 'No limit' (selected), 'Monthly limit' (with a text input for '(Mbytes)'), and 'Connection time control' (with a text input for '(Hours)'). The 'Traffic Counter' section allows setting a 'Restart traffic counter at' time (0:00 am) on the '1st' day of each month, with a 'Restart Counter Now' button. The 'Traffic Control' section has a checkbox for 'Pop up a warning message' (set to 0 Mbytes/Minutes) and two checkboxes for 'When the monthly limit is reached': 'Turn the Internet LED to flashing green/amber' and 'Disconnect and disable the Internet connection'.

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

4. (Optional) Control the volume of Internet traffic.

You can use either the traffic volume control feature or the connection time control feature to accomplish this goal:

- Select the **Traffic volume control by** radio button and then select one of the following options:
 - **No Limit.** No restriction is applied when the traffic limit is reached.
 - **Download only.** The restriction is applied to incoming traffic only.
 - **Both Directions.** The restriction is applied to both incoming and outgoing traffic.
- Select the **Connection time control** radio button and enter the allowed hours in the **Monthly limit** field.

5. (Optional) If your ISP charges for extra data volume when you make a new connection, enter the extra data volume in MB in the **Round up data volume for each connection by** field.

6. In the Traffic Counter section, set up the traffic counter to begin at a specific time and date of each month.

If you want the traffic counter to start immediately, click the **Restart Counter Now** button.

7. In the Traffic Control section, specify whether a warning message is issued before the monthly traffic limit of MB or hours is reached.

By default, the value is **0** and no warning message is issued. You can select one of the following to occur when the traffic limit is reached:

- The Internet LED blinks green or amber.
- The Internet connection is disconnected and disabled.

8. Click the **Apply** button.

Your changes are saved.

➤ **To continue monitoring Internet traffic after the initial setup:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

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

3. In the Internet Traffic Statistics section, monitor the data traffic.

Period	Connection Time (hh:mm)	Traffic Volume (Mbytes)		
		Upload/Avg	Download/Avg	Total/Avg
Today	0:00	0.00	0.00	0.00
Yesterday	0:00	0.00	0.00	0.00
This week	0:00/0:00	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	0.00/0.00
Last month	0:00/0:00	0.00/0.00	0.00/0.00	0.00/0.00

- To update the Traffic Statistics section, click the **Refresh** button.

- To display more information about the data traffic on your router and to change the poll interval, click the **Traffic Status** button.

Traffic Status

Counting Period	Amount Used
3/31 days	0.00/0.00 Mbytes

Poll Interval: (secs)

9. Troubleshooting

9

Diagnose and solve problems

This chapter provides information to help you diagnose and solve problems you might have with your router. If you do not find the solution here, visit the NETGEAR support site at <http://support.netgear.com> for product and contact information.

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshooting with the LEDs*
- *Cannot Log In to the Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *Wireless Connectivity*
- *Restore the Factory Settings and Password*
- *Troubleshoot Your Network Using the Ping Utility*

Quick Tips

This section describes tips for troubleshooting some common problems.

Sequence to Restart Your Network

Be sure to restart your network in this sequence:

1. Turn off *and* unplug the modem.
2. Turn off the router and computers.
3. Plug in the modem and turn it on. Wait two minutes.
4. Turn on the router and wait two minutes.
5. Turn on the computers.

Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in.

The Internet LED on the router is lit when the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.

For each powered-on computer connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED is lit.

Wireless Settings

Make sure that the wireless settings in the computer and router match exactly.

For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer need to match exactly.

If you set up an access list in the Advanced Wireless Settings screen, you must add each wireless computer's MAC address to the router's access list.

Network Settings

Make sure that the network settings of the computer are correct.

Wired and wirelessly connected computers need to have network (IP) addresses on the same network as the router. The simplest way to set this up is to configure each computer to obtain an IP address automatically using DHCP.

Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen.

Troubleshooting with the LEDs

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

1. When power is first applied, verify that the Power/Check LED is lit.
2. Verify that the Power/Check LED turns amber within a few seconds, indicating that the self-test is running.
3. After approximately 30 seconds, verify the following:
 - The Power/Check LED is solid green.
 - The Internet LED is lit.
 - A numbered Ethernet port LED on the back of the router is on for any local port that is connected to a computer. This activation indicates that a link has been established to the connected device.

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

Power/Check LED Is Off or Blinking

Make sure that the power cord is securely connected to your router and that the power adapter is securely connected to a functioning power outlet.

Make sure that you are using the power adapter that NETGEAR supplied for this product.

If the Power/Check LED blinks slowly and continuously, the router firmware is corrupted. This corruption can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. If the error persists, you have a hardware problem. For recovery instructions or help with a hardware problem, contact technical support at <http://support.netgear.com/general/contact/default.aspx>.

Power/Check LED Stays Amber

When the router is turned on, the Power/Check LED turns amber for about 20 seconds and then turns green. If the LED does not turn green, the router has a problem.

If the Power/Check LED is still amber one minute after you turn on power to the router, so the following:

1. Turn the power off and back on to see if the router recovers.
2. Press and hold the **Restore Factory Settings** button to return the router to its factory settings. See *Restore the Factory Settings and Password* on page 151.

If the error persists, you might have a hardware problem and should contact technical support at www.netgear.com/support.

LEDs Never Turn Off

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

If all LEDs are still on 1 minute after power-up, do the following:

- Cycle the power to see if the router recovers.
- Press and hold the **Restore Factory Settings** button to return the router to its factory settings. See *Restore the Factory Settings and Password* on page 151.

If the error persists, you might have a hardware problem and should contact technical support at www.netgear.com/support.

Internet or Ethernet LAN Port LEDs Are Off

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

- Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.
- Make sure that power is turned on to the connected modem or computer.
- Be sure that you are using the correct cable.

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

Wireless LEDs Are Off

If the Wireless LEDs stay off, check to see if someone pressed the **Wireless On/Off** button on the router. This button turns the wireless radios in the router on and off. The Wireless LEDs are lit when the wireless radio is turned on.

WPS/FastLane Button Blinks Amber

If, after you use the WPS/FastLane function, the button blinks amber, check the following:

- Make sure that you are using the button and not the router's built-in registrar.
- Check that PIN verification succeeded for the wireless device that you are adding to the wireless network.
- Make sure that you have not pressed the **WPS/FastLane** button on the front of the router after disabling the WPS/FastLane feature (you logged in to the router and disabled this feature previously).
- Check that the router is not in the temporary AP setup locked state (if you are using the wireless repeater function).

Cannot Log In to the Router

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router. For more information, see [Check Ethernet Cable Connections](#) on page 144.
- Make sure that your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address is in the range of 192.168.1.2 to 192.168.1.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. For more information, see [Factory Default Settings](#) on page 154.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. 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 factory default login name is *admin* and the password is *password*. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your NETGEAR router as an additional router behind an existing router in your network, consider replacing the existing router instead. NETGEAR does not support such a configuration.
- If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services, for example, converting ADSL or cable data into Ethernet networking information. NETGEAR does not support such a configuration.

Cannot Access the Internet

If you can access your router but you are unable to access the Internet, first determine whether the router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful.

➤ To check the WAN IP address:

1. Start your browser and navigate to an external site such as www.netgear.com.
2. Access the router interface at www.routerlogin.net.

For more information, see *Use NETGEAR genie after Installation* on page 17.

3. Select **ADVANCED > Administration > Router Status**.
4. Check that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network. See *Sequence to Restart Your Network* on page 144.

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

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

If your router 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:

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

Troubleshooting PPPoE

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

➤ **To troubleshoot a PPPoE connection:**

1. Log in to the router.

For more information, see *Use NETGEAR genie after Installation* on page 17.

2. Select **ADVANCED > Administration > Router Status**.
3. Click the **Connection Status** button. If all of the steps IP address and time information, your PPPoE connection is working.

If any of the steps indicate failure, you can attempt to reconnect by clicking the **Connect** button. The router continues to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There might be a provisioning problem with your ISP also.

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

Troubleshooting Internet Browsing

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

- Your computer might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.

Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, restart your computer.

Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

- Your computer might not have the router configured as its default gateway.

Reboot the computer and verify that the router address (www.routerlogin.net) is the default gateway address of your computer.

- You might be running login software that is no longer needed. If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select the **Never dial a connection** radio button.

Changes Not Saved

If the router does not save the changes you make in the router interface, check the following:

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

Wireless Connectivity

If you are having trouble connecting wirelessly to the router, check the following to try to isolate the problem:

- Does the wireless device or computer that you are using find your wireless network?
If not, check the Wireless LEDs on the front of the router. They should be lit. If they are not, you can press the **Wireless On/Off** button on the front of the router to turn the router's wireless radios back on.
If you disabled the router's SSID broadcast, then your wireless network is hidden and does not show up in your wireless client's scanning list. By default, SSID broadcast is enabled.
- Does your wireless device support the security that you are using for your wireless network? For example, does your wireless device support WPA2 security? If not, then you must change the security of the router to match the security that is supported by your wireless device. For more information, see [Basic Wireless Settings](#) on page 25.



WARNING:

NETGEAR recommends that you use the WPA2 wireless security option. Do not disable wireless security!

If your wireless device does not support WPA2 security, you might want to consider upgrading your wireless device to a newer model.

- If you want to view the wireless settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, and select **BASIC > Wireless**. For more information, see [Basic Wireless Settings](#) on page 25.

Note: *Be sure to click the **Apply** button when you make changes.*

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

- Is your router too far from your computer, or too close? Place your computer near the router, but at least 6 feet (2 meters) away, and see whether the signal strength improves.

- Is your wireless signal blocked by objects between the router and your computer?

Restore the Factory Settings and Password

This section explains how to restore the factory settings, changing the router's administration password back to **password**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router. For more information, see *Erase* on page 103.
- Use the **Restore Factory Settings** button on the bottom of the router. For more information, see *Factory Default Settings* on page 154. If you restore the factory settings and the router fails to restart, or the green Power/Check LED continues to blink, the unit might be defective. If the error persists, you might have a hardware problem and should contact technical support at <http://www.netgear.com/support>.

Troubleshoot Your Network Using the Ping Utility

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

Test the LAN Path to Your Router

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

➤ To ping the router from a running Windows computer:

1. From the Windows toolbar, select **Start > Run**.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:
ping www.routerlogin.net
3. Click the **OK** button.

You should see a message like this one:

```
Pinging <IP address > with 32 bytes of data
```

If the path is working, you see this message:

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

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

```
Request timed out
```

If the path is not functioning correctly, you might have one of the following problems:

- Wrong physical connections

For a wired connection, make sure that the numbered LAN port LED is on for the port to which you are connected.

Check that the appropriate LEDs are on for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are on for the switch ports that are connected to your computer and router.

- Wrong network configuration

Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, select **Start > 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 ISP DNS server.

If the path is functioning correctly, replies like the examples shown in [Test the LAN Path to Your Router](#) on page 151 are displayed. If you do not receive replies, check the following:

- Check that your computer has the IP address of your router listed as the default gateway. 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 router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Internet Setup screen.
- Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.

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

A Supplemental Information



Factory settings and technical specifications

This appendix provides factory default settings and technical specifications for the router.

- *Factory Default Settings*
- *Specifications*

Factory Default Settings

Table 3. Router default settings

Feature	Default Setting
Router login URL	http://www.routerlogin.net or http://www.routerlogin.com
Login name (case-sensitive)	admin (printed on product label)
Login password (case-sensitive)	password (printed on product label)
WAN MAC address	Default hardware address (printed on product label)
MTU size	1500
LAN IP address (gateway IP address)	192.168.1.1 (printed on product label)
Router subnet	255.255.255.0
DHCP server	Enabled
DHCP range	192.168.1.2 to 192.168.1.254
Time zone	GMT or other time zone settings based on your product SKU
Adjust for daylight saving time	Disabled
Allow a registrar to configure this router	Enabled
Wireless communication	Enabled
Preset SSID	NETGEARxx (xx refers to two random digits)
Security option password	Preset password (printed on product label)
Wireless access list (MAC filtering)	All wireless stations allowed
Broadcast SSID	Enabled
Transmission speed	Auto Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.
Country/Region	United States in NA only; otherwise, varies by country and region
RF channel	Auto until region selected
Operating mode	2.4 GHz 300 Mbps and 5 GHz 450 Mbps
Data rate	Best
Output power	Full

Table 3. Router default settings (continued)

Feature	Default Setting
Inbound communication from the Internet	Disabled (bars unsolicited requests except traffic on port 80, the HTTP port)
Outbound communication to the Internet	Enabled (all)

Specifications

Table 4. Router technical specifications

Feature	Specification
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, and UPnP
Power adapter	• North America: 110V, 60 Hz, input • UK, Australia: 240V, 50 Hz, input • Europe: 230V, 50 Hz, input • China: 220V, 60 Hz, input • All regions: 12 VDC @ 1.5A, output
Dimensions	217.74 x 147.73 x 34.92 mm 8.57 x 5.81 x 1.37 in.
Weight	392.6 g 0.87 lb
Operating temperature	0° to 40°C (32° to 104°F)
Operating humidity	90% maximum relative humidity, noncondensing
Designed to conform to the following standards	CCC SRRC CE
LAN	10BASE-T, 1000BASE-T, or 100BASE-Tx, RJ-45
WAN	10BASE-T , 1000BASE-T, or 100BASE-Tx, RJ-45

Index

A

- access control, turning on **112**
- access point (AP) mode **112**
- accessing remote computer **118**
- active static route **134**
- address reservation **50**
- advertisement period, UPnP **138**
- AES (Advanced Encryption Standard) **28**
- alerts, emailing **89**
- ALG (Application Layer Gateway) **44**
- applications, QoS for **56**
- approved USB devices **67, 74**
- attached devices **32**
- authentication, required by mail server **90**
- automatic firmware checking **104**
- automatic Internet connection **41**

B

- back panel **12**
- backing up configuration **102, 103**
- bandwidth control, QoS **53**
- base station, wireless distribution system **115**
- blocking
 - inbound traffic **118**
 - keywords and sites **85, 86**
 - services **87**
- box contents **8**

C

- cables, checking **144**
- changes not saved **150**
- channel, wireless **26**
- configuration file **101**
- connecting wirelessly, operating range **9**
- connection status **96**
- country setting **40**
- crossover cable **146**
- CTS/RTS Threshold **107**
- custom service, port forwarding **123**

D

- data packets, fragmented **45**
- default DMZ server **44**
- default factory settings, restoring **103, 151**
- default gateway **97**
- denial of service (DoS) protection **43, 84**
- devices, attached **32**
- DHCP server **49, 97**
- DMZ server **44, 45**
- DNS addresses
 - setting **25, 113**
 - troubleshooting **148**
 - viewing **94, 97**
- Dynamic DNS **131**
- DynDNS.org **131**

E

- email notices **89**
- erasing configuration **103**
- Ethernet cables, checking **144**
- Ethernet LEDs, troubleshooting and **145**

F

- factory default settings, restoring **103, 151**
- FastLane **38**
- file sharing **75**
- firmware version **93**
- firmware, upgrading **18, 104**
- fragmentation length **107**
- fragmented data packets **45**
- front panel **10**

G

- gateway IP address **25, 113**
- gateway, default **97**
- genie, NETGEAR
 - logging in **17**
 - setup, initial **16**
- guest networks **36**

H

hardware version **93**
 hops, UPnP **139**
 host name **24**
 host, trusted **86**

I

IGMP proxy **44**
 inbound traffic, blocking **118**
 installing **16, 17, 40**
 Internet connection
 setting up **24**
 status **96**
 troubleshooting **16, 147**
 Internet LED
 described **11**
 troubleshooting and **145, 146**
 Internet port
 back panel **12**
 Setup Wizard **41**
 viewing settings **93**
 Internet Relay Chat (IRC) **120**
 Internet service provider (ISP) **15**
 Internet services, blocking access **87**
 IRC (Internet Relay Chat) **120**

K

keywords **85, 86**

L

label, product **13**
 LAN port LEDs
 described **11**
 troubleshooting and **146**
 LAN ports
 back panel **12**
 viewing settings **93**
 LAN setup **47**
 language setting **40**
 large files, sharing **76**
 lease, DHCP **97**
 LEDs
 described **11**
 troubleshooting and **145, 146**
 Live Parental Controls **33**
 local servers, port forwarding to **122**
 logging in **15, 17**
 logs **89**

M

MAC addresses
 product label **13**
 QoS for **58, 59**
 mail server, outgoing **90**
 maintenance settings **91**
 metric values, static routes **135**
 mixed mode wireless security option **28**
 mode, wireless **27**
 MTU size **45**
 multicasting **48**

N

NAT (Network Address Translation) **43, 44**
 NETGEAR genie
 logging in **17**
 setup, initial **16**
 networks
 guest **36**
 restarting **144**
 troubleshooting **144**

O

online games, QoS for **56**
 open NAT **44**
 outgoing mail server **90**

P

packets
 fragmented **45**
 transmitted and received **95**
 parental controls **33**
 passphrases
 changing **29**
 product label **13**
 passwords
 recovering **19**
 restoring **151**
 photos, sharing **76**
 Point-to-Point Tunneling Protocol (PPTP), connection
 status **97**
 policies, QoS **54**
 port filtering **87**
 port forwarding **118, 121, 122**
 port numbers **87**
 port triggering **118, 120, 122, 127**
 portmap table, UPnP **139**
 ports

- listed, back panel **12**
 - status, viewing **95**
- positioning the router **9**
- Power On/Off button, back panel **12**
- Power port, back panel **12**
- Power/Check LED
 - described **11**
 - troubleshooting and **145**
- PPPoE (PPP over Ethernet)
 - connection status **97**
 - troubleshooting and **148**
- PPTP (Point-to-Point Tunneling Protocol), connection status **97**
- Preamble mode **107**
- preset security
 - about **25**
 - passphrase **29**
- primary DNS addresses **25, 113**
- printing files and photos **76**
- prioritizing traffic **52, 59, 61**
- private static route **134**
- protection, Internet **33**
- Push 'N' Connect **21**

Q

QoS (Quality of Service) **52–54**

R

- RADIUS server **29**
- range of wireless connections **9**
- ReadySHARE access **66, 78**
- received packets **95**
- recovering administrative password **19**
- releasing and renewing connection status **97**
- repeater, wireless distribution system **116**
- reserved IP addresses **48, 50**
- restarting network **144**
- restoring default factory settings **103, 151**
- RIP (Router Information Protocol)
 - setting up **48**
 - static routes **134**
- router status, viewing **92**
- rules, QoS **54**

S

- scheduling keyword and service blocking **89**
- secondary DNS **25, 113**
- secured NAT **44**

- security **25**
 - firewall settings **84**
 - wireless settings **31**
- security PIN **42**
- sending logs by email **89**
- serial number, product label **13**
- services
 - blocking **87**
 - port forwarding **123**
 - port triggering **129**
- Session Initiation Protocol Application Layer Gateway (SIP ALG) **44**
- Setup Wizard **40, 41**
- shared key, WEP **31**
- sharing files **75**
- SIP ALG (Session Initiation Protocol Application Layer Gateway) **44**
- sites, blocking **85, 86**
- SMTP server **90**
- software version **93**
- specifications, technical **153**
- SSID
 - broadcasting **27, 36**
 - described **26, 36**
 - product label **13**
- static routes **132**
- statistics, traffic **94**
- status, connection **96**
- system up time **95**

T

- technical specifications **153**
- technical support **2**
- Temporal Key Integrity Protocol (TKIP) **28**
- time to live, advertisement, UPnP **139**
- time-out, port triggering **128**
- TKIP (Temporal Key Integrity Protocol) **28**
- trademarks **2**
- traffic
 - metering **139**
 - prioritizing **52, 59, 61**
 - statistics, viewing **94**
- transmitted packets **95**
- troubleshooting **143, 147, 150**
- trusted host **86**

U

- up time, system **95**
- upgrading firmware **18, 104**

uplink bandwidth [53](#)

USB

advanced configuration [68](#)

drive requirements [66](#)

file sharing [75](#)

ReadySHARE access [66](#), [78](#)

remote computer connection [78](#)

specifying approved devices [74](#)

unmounting USB drive [66](#)

UPnP [138](#)

USB devices, approved [67](#), [74](#)

USB LED [11](#)

user-defined services [87](#)

checking for correct [144](#)

described [26](#), [36](#), [99](#)

viewing [98](#)

WMM (Wi-Fi Multimedia) [52](#)

WPA/WPA2 Enterprise [30](#)

WPA-PSK, WPA2-PSK, and WPA+WPA2 mixed mode
[28](#)

WPS/FastLane button [12](#), [22](#)

WPS/FastLane LED

described [11](#)

troubleshooting and [146](#)

V

versions, firmware, hardware, and language [93](#)

VoIP (Voice over IP) [44](#)

W

WAN IP address, troubleshooting [147](#)

WAN port

back panel [12](#)

viewing settings [93](#)

WAN setup [43](#)

web server, port forwarding [126](#)

WEP (Wired Equivalent Privacy) [30](#)

Wi-Fi Multimedia (WMM) [52](#)

Wi-Fi Protected Setup (WPS) [21](#), [42](#)

devices, adding [21](#)

keep existing settings [110](#)

Wired Equivalent Privacy (WEP) [30](#)

Wireless Card Access List [111](#)

wireless channel [26](#)

wireless connections

operating range [9](#)

troubleshooting [150](#)

wireless devices, adding to the network [21](#)

wireless distribution system [115](#), [116](#)

Wireless LEDs

described [11](#)

troubleshooting and [146](#)

wireless mode [27](#)

wireless network name (SSID)

broadcasting [27](#), [36](#)

described [26](#), [36](#)

product label [13](#)

Wireless On/Off button [11](#)

wireless repeating [114](#)

wireless security options [27](#), [31](#), [37](#)

wireless settings