NETGEAR ®

D6200 WiFi Modem Router

User Manual

Note: This draft is a certification document and there might be some differences between this user manual and the actual unit.

Support

Thank you for choosing NETGEAR.

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 web site. For product updates and web support, visit *http://support.netgear.com*.

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

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

NETGEAR recommends that you use only the official NETGEAR support resources.

Trademarks

Contents

Chapter 4   NETGEAR genie ADVANCED Home

Chapter 5   USB Storage

Chapter 6   USB Printer Control

Chapter 7   Security

Chapter 8 Administration

Chapter 9 Advanced Settings

Chapter 10 Troubleshooting

Appendix A Supplemental Information

Appendix B Notification of Compliance

Index

Hardware Setup

1

Get to know your wireless router

The NETGEAR D6200 WiFi Modem Router offers maximum-performance wireless speeds of up to 450 Mbps needed for demanding applications, such as large file transfers, streaming HD video, and multiplayer gaming. Complete with a built-in DSL modem, it is compatible with all major DSL Internet service providers. Simultaneous dual-band technology runs both 2.4 GHz and 5 GHz bands at the same time, ensuring top speeds and the greatest range, while Gigabit offers ultrafast wired connections. The unit supports a wide range of premium features and applications such as ReadySHARE® Cloud, ReadySHARE® Printer, and NETGEAR genie.

- **All-in-one**. Built-in ADSL2+ modem and WAN Gigabit Ethernet port for cable or fiber combined with a wireless router create an integrated home gateway.

- **ReadySHARE Cloud**. Access and share files on an attached USB hard drive anywhere you have an Internet connection.

- **ReadySHARE Printer**. Wirelessly print from your Mac or Windows computer to a connected USB printer.

- **ReadySHARE USB**. Wirelessly share a USB hard drive with Macs and PCs.

- **Faster multimedia streaming**. Provides up to 450 Mbps wireless speed for streaming HD videos, simultaneous downloads, and online gaming in addition to basic Internet applications.

- **Simultaneous dual band**. Runs both 2.4 GHz and 5 GHz bands concurrently, ensuring top speeds and the greatest range while minimizing interference.

- **NETGEAR genie**. Easy setup and dashboard control to manage, monitor, and repair home networks.

- **Ultrafast wired**. Four Gigabit Ethernet ports deliver ultrafast wired connections for gaming and video.

- **Live Parental Controls**. Keeps your Internet experience safe using flexible and customizable filter settings.

- **Guest network access**. Provides separate security and access restrictions for guests using the network.

- **Broadband usage meter**. Monitors Internet traffic and sends customized reports to help keep costs under control.

- **Secured connection**. Push 'N' Connect ensures a quick and secure network connection.

- **NETGEAR green features**. Use Power and WiFi On/Off buttons, and schedule WiFi to turn on and off to save energy when not in use.

- **Compatibility**. Compatible with all major ADSL Internet service providers (ISPs).

Product Specifications

Package Contents

- D6200 WiFi Modem Router
- Ethernet cable
- Phone cable and filter
- Power adapter, localized to country of sale

Warranty

- Localized to country of sale

System Requirements

- Broadband Internet service
    - ADSL broadband Internet service
    - Cable or fiber. Connects to cable modem or fiber termination node through the Gigabit Ethernet WAN port
- 802.11-a/b/g/n 2.4 GHz or 5.0 GHz specification wireless adapter or an Ethernet adapter and cable for each computer
- Microsoft Windows 7, Vista, XP, 2000, Me, Mac OS, UNIX, or Linux
- Microsoft Internet Explorer 5.0, Firefox 2.0, Safari 1.4, or later
- Use with an N600 Wireless Dual Band USB Adapter (WNDA3100 for maximum performance)

Standards

- IEEE 802.11-b/g/n 2.4 GHz
- IEEE 802.11-a/n 5.0 GHz
- Five (5) 10/100/1000 (1 WAN and 4 LAN) Gigabit Ethernet ports
- Two (2) USB 2.0 ports
- One (1) ADSL2+ port

Performance

- All-in-one. High-speed ADSL2+ modem (built-in) and WAN Gigabit Ethernet port for cable or fiber
- Powerful dual-core (400 MHz each) processor
- High-speed access to external USB storage using two USB 2.0 ports
- Memory. 128 MB flash and 128 MB RAM
- Five (5) (1 WAN, 4 LAN) Gigabit-Ethernet ports
- Advanced Quality of Service (QoS)

Security

- Wi-Fi Protected Access® (WPA/WPA2-PSK) and WEP
- Double firewall protection (SPI and NAT firewall)
- Denial of service (DoS) attack prevention

Ease of Use

- Easy installation. Connect to computer and open your browser to install
- Push 'N' Connect using Wi-Fi Protected Setup® (WPS)

Physical Specifications

- Dimensions: 205 x 255 x 77 mm (8.07 x 10.04 x 3.03 inches)
- Weight: 654g (1.44 lb)

Premium Features:

- ReadySHARE CLOUD. Access and share a USB hard drive remotely.
- ReadySHARE PRINTER. Wirelessly access and share a USB printer.

Advanced Features

- Live Parental Controls with flexible and customizable filter settings.
- Simultaneous dual band. 2.4 GHz and 5 GHz operation.
- Two (2) ports for ReadySHARE® USB storage access. Supports FAT16/32, NTFS Read/Write.
- DLNA®. Stream media to DLNA media players.
- Multiple SSID guest networks (separate security and access restrictions).
- Broadband usage meter measures Internet usage.
- Power and Wi-Fi On/Off buttons.

NETGEAR Green Features

Power On/Off button

80% recycled packaging

CEC (California Efficiency)

RoHS

WEEE

If you did not set up your new modem router already using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 3, NETGEAR genie BASIC Settings,* explains how to set up your Internet connection.

For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com/general/contact/default.aspx.*

This chapter contains the following sections:

- *Unpack Your New Router*
- *Hardware Features*

- *Position Your Wireless Router*
- *ADSL Microfilters*
- *Cable Your D6200 WiFi Modem Router*
- *Verify the Cabling*

Unpack Your New Router

Your box should contain the following items:

- D6200 WiFi Modem Router
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Microfilters and splitters (quantity and type vary by region)
- Installation guide with cabling and router setup instructions

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair. See *Position Your Wireless Router* on page 18 for information about where to place and how to position your router.

D6200
Modem Router

Ethernet cable

Telephone cable

Power adapter

Filter splitter

The filter or splitter provided depends on the region.
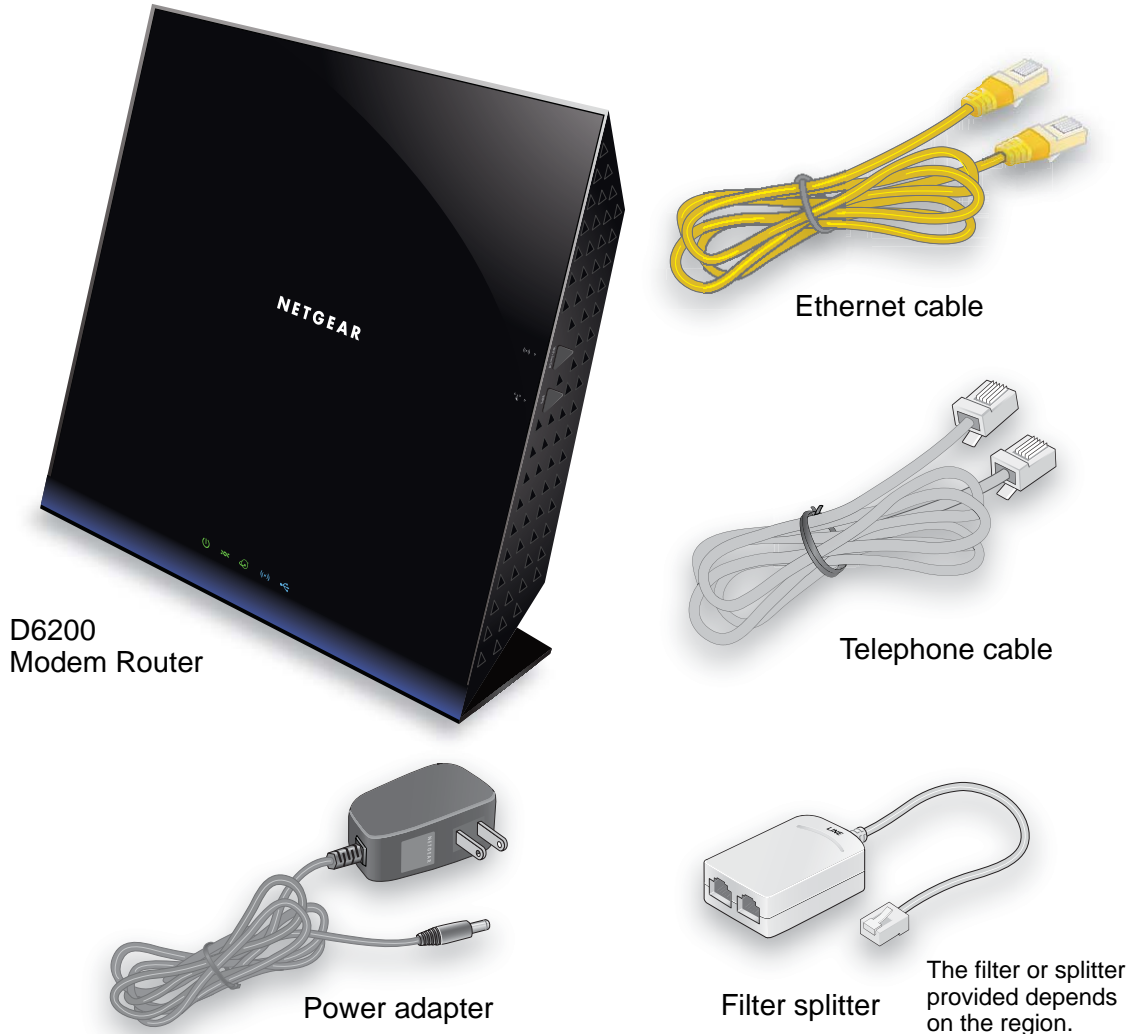
Figure 1. Box contents

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.

Label

The label on the bottom of the WiFi modem router shows the router's WiFi network name (SSID) and network key (password).
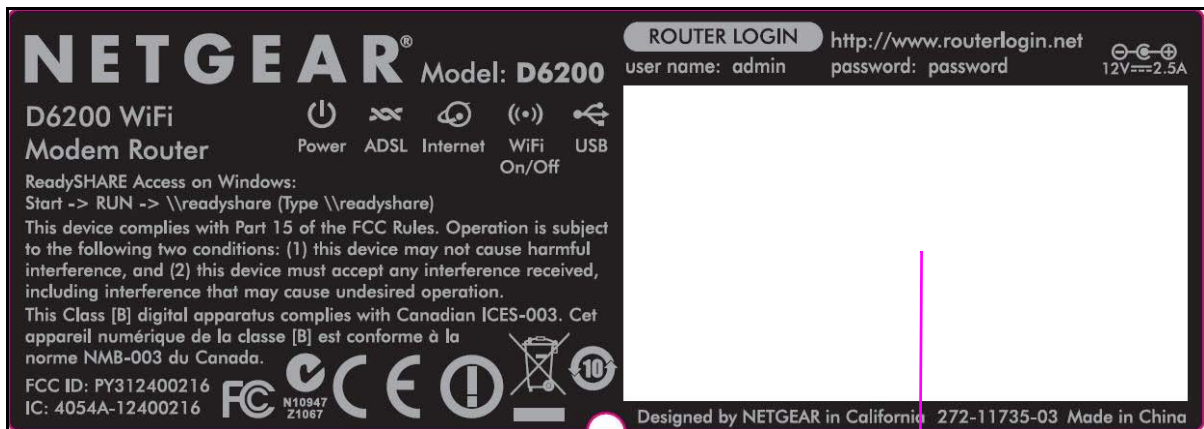
WiFi network name (SSID) and network key (password)

Figure 2. Label on router bottom

Back Panel

The back panel has the Power On/Off button and port connections shown in the figure:
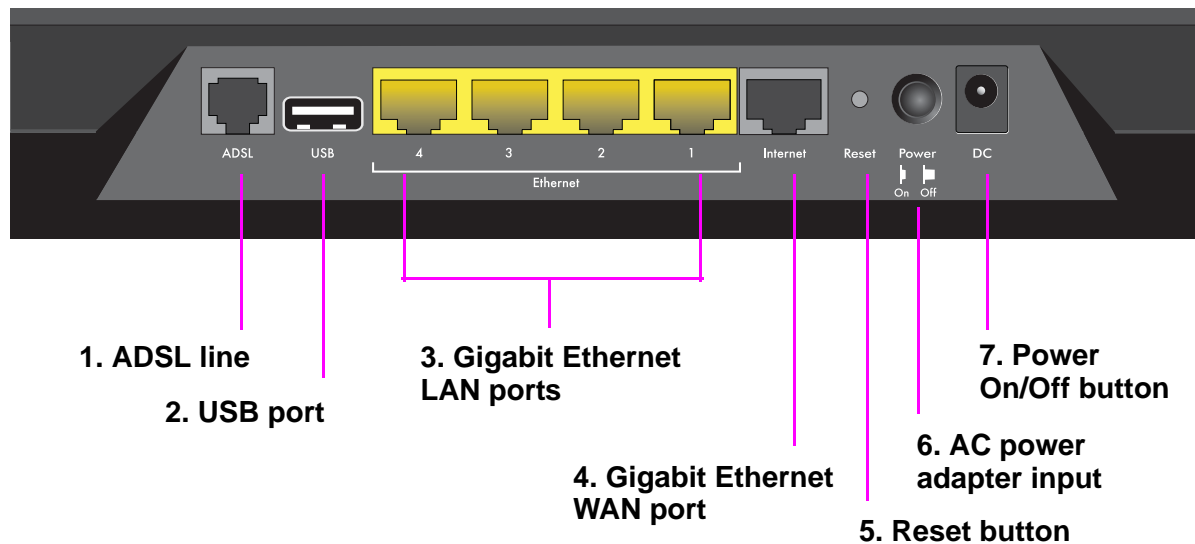
Figure 3. Back panel port connections

Viewed from left to right, the back panel contains the following elements:

1. RJ-11 asynchronous DSL (ADSL) port for connecting the WiFi modem router to an ADSL line

> **Note:** An ADSL port can send data over an ADSL line at one speed and receive it at another speed.

2. USB port for connecting USB storage devices like flash drives, hard drives, or USB printers

3. Four Gigabit Ethernet RJ-45 LAN ports for cabling the WiFi modem router to the local computers

4. One Gigabit Ethernet WAN port for connecting the WiFi modem router to a fiber or cable modem

> **Note:** You can use either the ADSL or Gigabit Ethernet port for WAN connectivity.

5. Reset button

   See *Factory Settings* on page 141 for information about the Restore Factory Settings button and the factory setting values.

6. Power On/Off button

7. AC power adapter input

Front Panel

The WiFi modem router front panel has the 5 status LEDs, icons, and ports shown in the figure.

Power   DSL   Internet   Wireless   USB
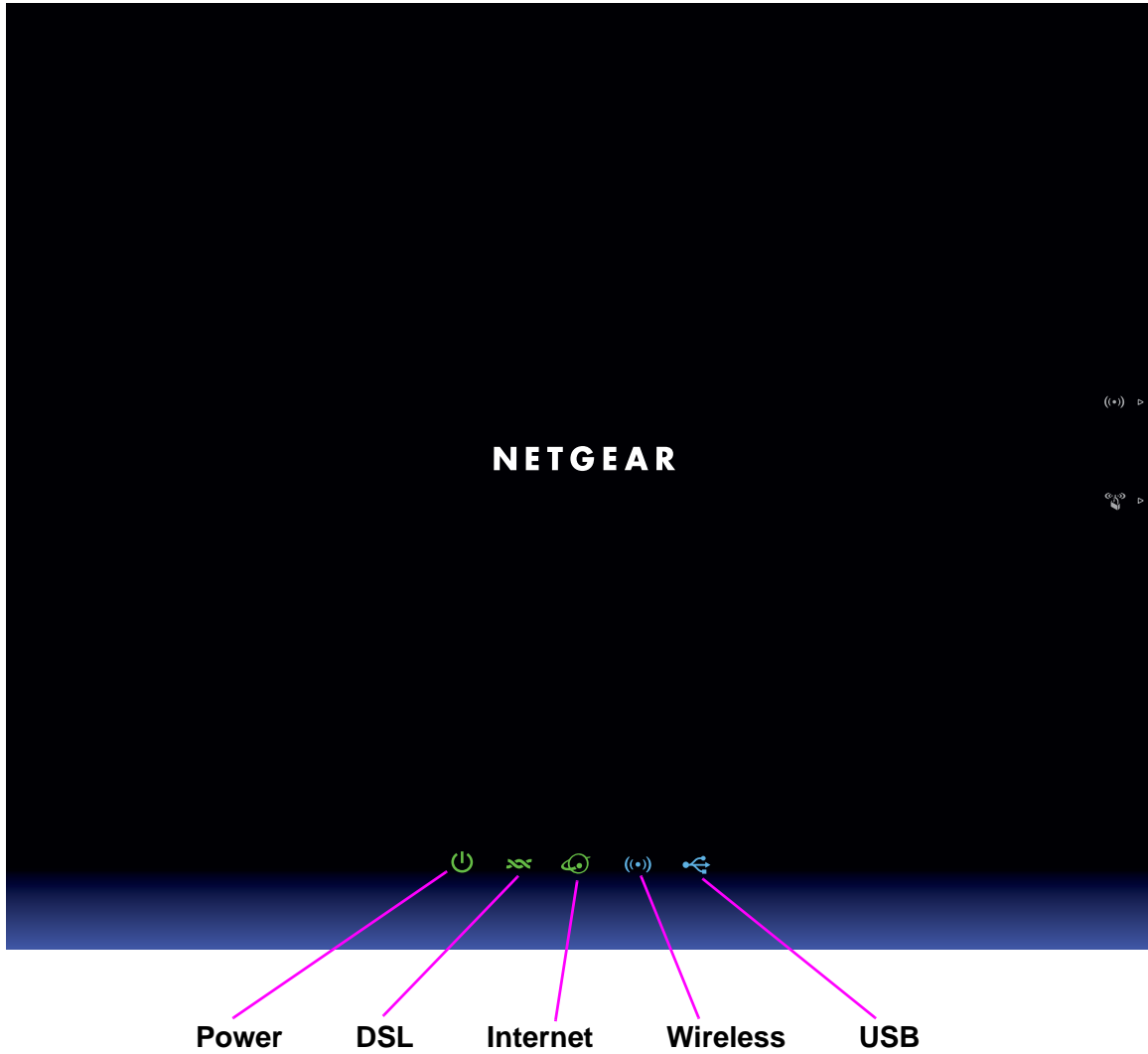
Figure 4. Front panel LEDs

The following tables describe the LEDs and icons on the front panel from left to right.

Table 1. Power On/Off LED

Icon	LED Activity	Description
	Solid green	Power is supplied to the router.
	Solid red	POST (power-on self-test) failure or a device malfunction occurred.
	Off	Power is not supplied to the router.
	Restore Factory Settings	LED blinks momentarily when the Restore Factory Settings button on the bottom of the unit is pressed for 6 seconds. The Power LED then blinks red three times when the Restore Factory Settings button is released and then turns green as the gateway resets to the factory defaults.

Table 2. DSL LED

Icon	LED Activity	Description
	Solid green	You have an ADSL connection. In technical terms, the ADSL port is synchronized with an ISP network-access device.
	Blinking green	Indicates that the WiFi modem router is negotiating the best possible speed on the ADSL line.
	Off	The unit is off or has no ADSL connection.

Table 3. Internet LED

Icon	LED Activity	Description
	Solid green	You have an Internet connection. If this connection is dropped due to an idle time-out but the connection is still present, the LED stays green. If the Internet connection is dropped for any other reason, the LED turns off.
	Solid red	The Internet (IP) connection failed. See *Cannot Access the Internet* on page 134 for troubleshooting information.
	Blinking green	Data is being transmitted over the Internet connection.
	Off	No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection).

Table 4. Wireless LED

Icon	LED Activity	Description
	Solid blue	There is wireless connectivity.
	Blinking blue	Data is being transmitted or received over a wireless link or a WPS-capable device is connecting to the device.
	Off	There is no wireless connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity.

Table 5. USB LED

Icon	LED Activity	Description
	Solid blue	A USB port detected a USB device.
	Blinking blue	Data is being transmitted or received.
	Off	No link is detected on these ports.

Side Panel

The WiFi modem router side panel has the port and buttons shown in the figure.

Wireless On/Off button

WPS On/Off button
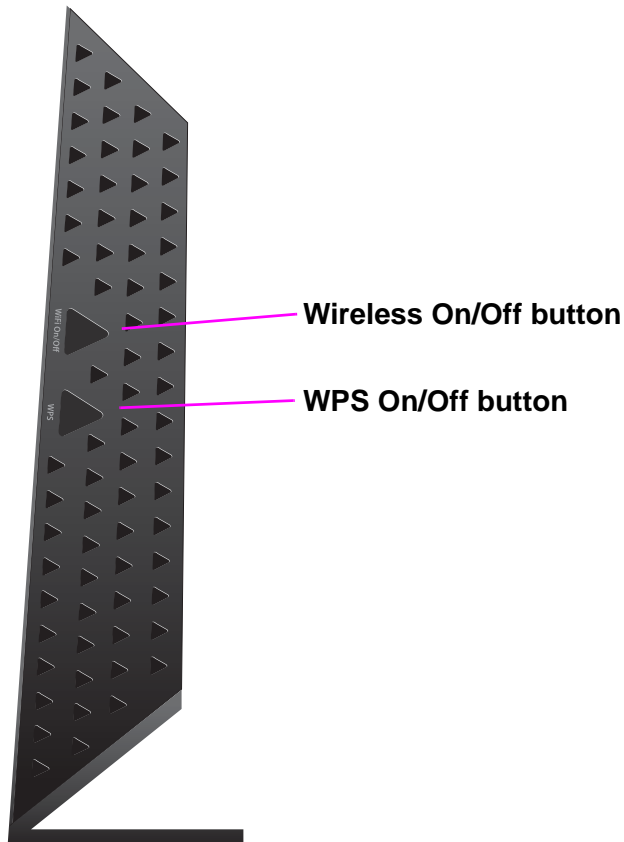
Figure 5. Side panel buttons and port

The following tables describe the buttons and port on the side panel from top to bottom.

Table 6. Wireless button

Icon	Description
	For information about the use of this button, see *Wireless Connectivity* on page 137.

Table 7. WPS button

Icon	Description
	For information about the use of this button, see *Wi-Fi Protected Setup (WPS) Method* on page 27.

Position Your Wireless Router

The WiFi modem router lets you access your network from 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. For best results, place your router:

- Near the center of the area where your computers and other devices operate and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the WiFi modem router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, computers, or the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

Note: The D6200 should be put in a vertical position only.

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

ADSL Microfilters

If this installation is the first time you have cabled a wireless router between an ADSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your D6200 WiFi Modem Router* on page 20.

An ADSL microfilter is a small inline device that filters ADSL interference out of standard phone equipment that shares line with your ADSL service. Every telephone device that connects to a telephone line that provides ADSL service needs an ADSL microfilter to filter out the ADSL interference. Example devices are telephones, fax machines, answering machines, and caller ID displays. Not every phone line in your home necessarily carries ADSL service. That depends on the ADSL service setup in your home.

> **Note:** Often the ADSL microfilter is included in the box with the wireless modem router. If you purchased the WiFi modem router in a country where a microfilter is not included, you have to acquire the ADSL microfilter separately.

One-Line ADSL Microfilter (Not Included)

Plug the ADSL microfilter into the wall outlet and plug your phone equipment into the jack labeled Phone. The wireless modem router plugs directly into a separate ADSL line. Plugging the wireless modem router into the phone jack blocks the Internet connection. If you do not have a separate ADSL line for the router, the best thing to do is to use an ADSL microfilter with a built-in splitter.

Plugs into ADSL line
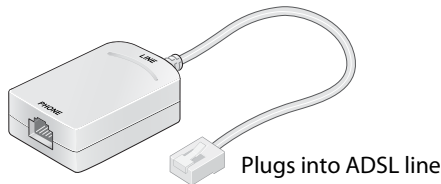
Figure 6. One-line ADSL microfilter

Second best when you do not have a separate ADSL line for the router is to get a separate splitter. To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

Two-Line ADSL Microfilter (Included)

Use an ADSL microfilter with a built-in splitter when there is a single wall outlet that provides connectivity for both the WiFi modem router and your telephone equipment. Plug the ADSL microfilter into the wall outlet, plug your phone equipment into the jack labeled Phone, and plug the wireless modem router into the jack labeled ADSL.

Plugs into the ADSL line
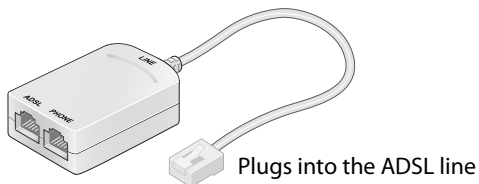
Figure 7. Two-line ADSL microfilter with built-in splitter

Summary

- One-line ADSL microfilter (not included). Use with a phone or fax machine.
- Splitter (not included). Use with a one-line ADSL microfilter to share an outlet with a phone and the WiFi modem router.

• Two-line ADSL microfilter with built-in splitter (included). Use to share an outlet with a phone and the WiFi modem router.

Cable Your D6200 WiFi Modem Router

⚠ **WARNING:**

Do not stack equipment or place equipment in tight spaces, in drawers, or on carpets. Be sure that your equipment is surrounded by at least 2 inches of air space. The unit should not be wall mounted.

The installation guide that came in the box has a cabling diagram on the second page.
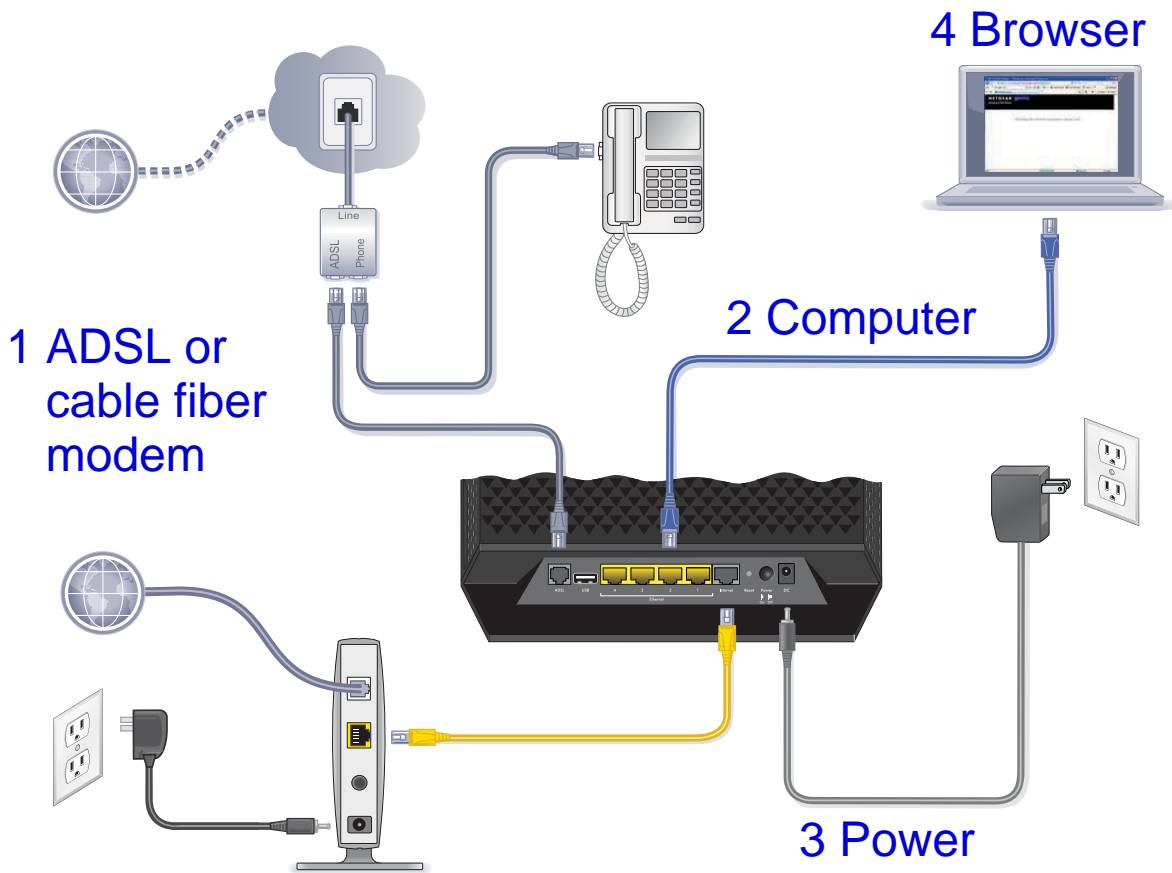
Figure 8. Cabling diagram

⚠ **CAUTION:**

Incorrectly connecting a filter to your WiFi modem router blocks your ADSL connection.

Verify the Cabling

Verify that your router is cabled correctly by checking the WiFi modem router LEDs. Turn on the wireless router by pressing the **Power On/Off** button on the back.

- The Power LED is green when the modem router is turned on.
- The Wireless LED is lit when the modem router is turned on.
- The DSL LED is green when you have an ADSL connection.
- The Internet LED is green when an Internet connection exists.

Turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically.

Get Started with NETGEAR genie 2

Connect to the WiFi modem router

This chapter explains how to use NETGEAR genie to set up your WiFi modem router after you complete cabling as described in the installation guide and in the previous chapter in this book.

This chapter contains the following sections:

- *Prepare to Set Up the WiFi Modem Router*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie after Installation*
- *Upgrade WiFi Modem Router Firmware*
- *WiFi Modem Router Dashboard (BASIC Home Screen)*
- *Add Wireless Devices or Computers to Your Network*

Prepare to Set Up the WiFi Modem Router

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

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

If you have DSL broadband service, you might need the following information to set up your WiFi modem router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. 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 WiFi modem router automatically logs you in.

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

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 WiFi modem router. See *Basic Wireless Settings* on page 35 for information about the WiFi modem router's preconfigured security settings.

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.

- **Wireless modem router login** logs you in to the WiFi modem router interface from NETGEAR genie. See *Use NETGEAR genie after Installation* on page 25 for details about this login.

Wireless network key or password. Your WiFi modem router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label on the bottom of your WiFi modem router.

- **ISP login** logs you in to your Internet service. Your service provider provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.

NETGEAR genie Setup

NETGEAR genie runs on any device with a web browser. It is the easiest way to set up the WiFi modem 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 WiFi modem router:**

1. Turn the WiFi modem router on by pressing the **On/Off** button, if not done yet.
2. Make sure that your device is connected with an Ethernet cable to your WiFi modem router.
3. Launch your Internet browser.
   - If this installation is the first time you are setting up the Internet connection for your WiFi modem 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 25.
4. Follow the onscreen instructions to complete NETGEAR genie setup. NETGEAR genie guides you through connecting the WiFi modem router to the Internet.

➢ **If the browser cannot display the web page:**

- Make sure that the computer is connected to one of the 4 Gigabit Ethernet LAN ports, or wirelessly to the WiFi modem router.
- Make sure that the WiFi modem router is ready. Its Wireless LEDs should light.
- Close and reopen the browser to make sure that the browser does not cache the previous page.
- Browse to **http://routerlogin.net**.
- If your computer is set to a static or fixed IP address (this situation is uncommon), change the setting to obtain an IP address automatically from the WiFi modem router.

➢ **If the WiFi modem router does not connect to the Internet:**

1. Review your settings to be sure that you selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 10, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR technical support.

Use NETGEAR genie after Installation

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

1. Launch your browser from a computer or wireless device that is connected to the WiFi modem router.

2. Enter **http://www.routerlogin.net** in the web browser address bar.

   A login window displays.

3. Enter **admin** for the WiFi modem router user name and **password** for the WiFi modem router password, both in lowercase letters.

   Note: The WiFi modem router user name and password are different from the user name and password for logging in to your Internet connection. See *Types of Logins and Access* on page 23 for more information.

Upgrade WiFi Modem Router Firmware

When you set up your WiFi modem router and are connected to the Internet, the WiFi modem 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. See *Upgrade the WiFi Modem Router Firmware* on page 85 for more information about upgrading firmware.

Click the message when it shows up, and click **Yes** to upgrade the WiFi modem router with the latest firmware. After the upgrade, the WiFi modem router restarts.

⚠ **CAUTION:**

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

WiFi Modem Router Dashboard (BASIC Home Screen)

The WiFi modem router BASIC Home screen has a dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the six sections of the dashboard to view more detailed information. Menus are on the left, and the Advanced tab that is used to access additional menus and screens is at the top.

Figure 9. Wireless modem router BASIC Home screen with dashboard, language, and online help

- **Home**. This dashboard screen displays when you log in to the WiFi modem router.
- **Internet**. Set, update, and check the ISP settings of your WiFi modem router.
- **Wireless**. View or change the wireless settings for your WiFi modem router.
- **Attached Devices**. View the devices connected to your network.
- **Parental Controls**. Download and set up parental controls to prevent objectionable content from reaching your computers.

- **ReadySHARE**. If you connected a USB storage device to the WiFi modem router, then it is displayed here.
- **Guest Network**. Set up a guest network to allow visitors to use your WiFi modem router's Internet connection.
- **Advanced tab**. Set the WiFi modem router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 9, Advanced Settings*. Using this tab requires a solid understanding of networking concepts.
- **Help & Support**. Go to the NETGEAR support site to get information, help, and product documentation. These links work after you have an Internet connection.

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. See *Guest Networks* on page 38 for instructions for how to set up a guest network.

Manual Method

➢ **To connect manually:**

1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your WiFi modem router. The wireless software scans for all wireless networks in your area.

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

3. Enter the WiFi modem router password and click **Connect**. The default WiFi modem router passphrase is on the product label on the bottom of the WiFi modem router.

4. Repeat steps 1–3 to add other wireless devices.

Wi-Fi Protected Setup (WPS) 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 WiFi modem router so that every device in the network has the same security settings.

If your wireless device supports WPS (Push 'N' Connect), use the following procedure.

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

1. Press the **WPS** button on the WiFi modem router top panel.

2. Within 2 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 WiFi modem router.

3. Repeat steps 1–2 to add other WPS wireless devices.

NETGEAR genie BASIC Settings

3

Your Internet connection and network

This chapter explains the features available from the NETGEAR genie BASIC Home screen, shown in the following figure:
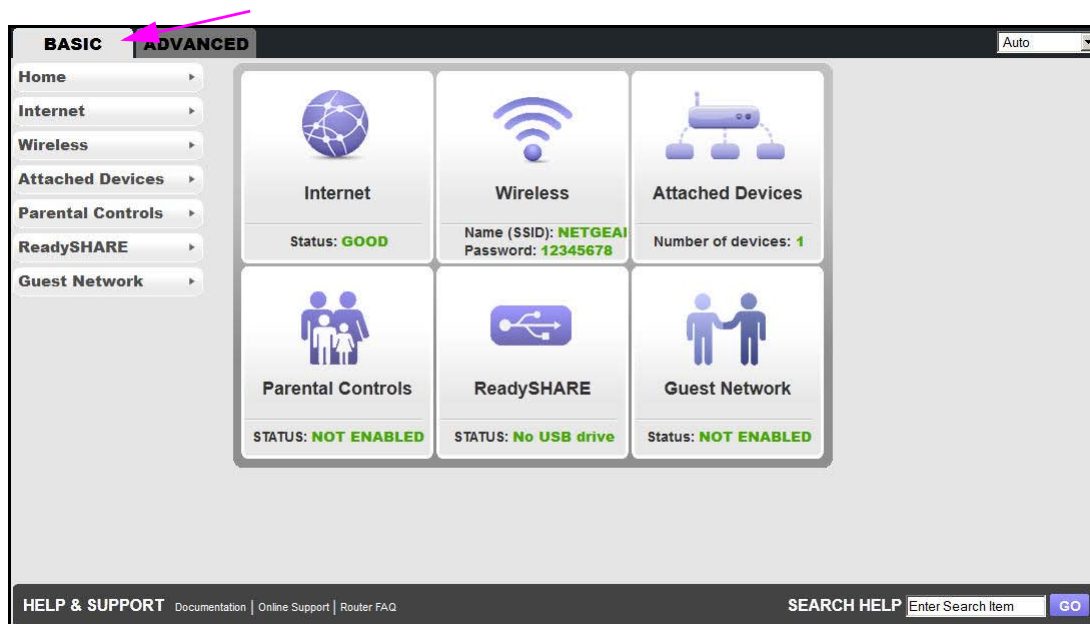
This chapter contains the following sections:

- *Internet Basic Settings*
- *Attached Devices*
- *Parental Controls*
- *ReadySHARE USB Storage and Printer*
- *Basic Wireless Settings*
- *Guest Networks*
- *NETGEAR genie App*

Internet Basic Settings

The Internet Basic Settings screen is where you view or change ISP information.

1. From the BASIC Home screen, select **Internet**. The following screen displays:

Scroll to view more settings

The fields that display in the Internet Basic Settings screen depend on whether your Internet connection requires a login.

- **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.

2. 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.

3. Click **Apply** to save your settings.

4. Click **Test** to test your Internet connection. If the NETGEAR website does not display within 1 minute, see *Chapter 10, Troubleshooting*.

Internet Basic Settings Screen Fields

The following descriptions explain all of the possible fields in the Internet Basic Settings screen. Which fields display in this screen depends on whether an ISP login is required.

Does Your ISP Require a Login? Answer either yes or no.

These fields display when no login is required:

- **Account Name (If Required)**. Enter the account name provided by your ISP. This name 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 Encapsulation**. ISP types. The choices are PPPoE or PPPoA.
- **Login**. The login name provided by your ISP. This name is often an email address.
- **Password**. The password that you use to log in to your ISP.
- **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 WiFi modem router keeps the Internet connection active after no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- **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 WiFi modem router to which your WiFi modem router connects.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

- **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 does not automatically transmit DNS addresses to the WiFi modem router during login, select this option, and enter the IP address of your ISP primary DNS server. If a secondary DNS server address is available, enter it also.

WiFi Modem Router MAC Address. The Ethernet MAC address used by the WiFi modem router 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 then accept traffic only from the MAC address of that computer. This feature allows your WiFi modem router to use your computer's MAC address (this procedure is also called cloning).

- **Use Default Address**. Use the default MAC address.
- **Use Computer MAC Address**. The WiFi modem router captures and use 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.

Attached Devices

You can view all computers or devices that are currently connected to your network here. From the Basic Home screen, select **Attached Devices** to display the following screen:

Wired devices are connected to the WiFi modem router with Ethernet cables. Wireless devices have joined the wireless network.

- **#** (number). The order in which the device joined the network.
- **IP Address**. The IP address that the WiFi modem router assigned to this device when it joined the network. This number can change when a device is disconnected and rejoins the network.
- **Device Name**. If the device name is known, it is shown here.
- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.

You can click **Refresh** to update this screen.

Parental Controls

The first time you select Parental Controls from the BASIC Home screen, you are automatically directed to the Internet, where you can learn more about Live Parental Controls or download the application. The following screen displays:
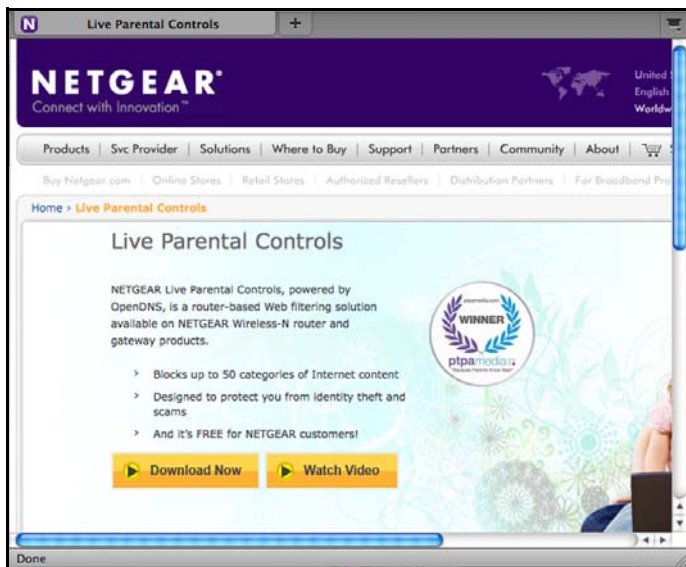
ReadySHARE USB Storage and Printer

You can view information about a USB storage device that is connected to the WiFi modem router's USB port here.

USB Storage (Basic Settings)

From the Basic Home screen, select **ReadySHARE** to display the USB Storage (Basic Settings) screen:
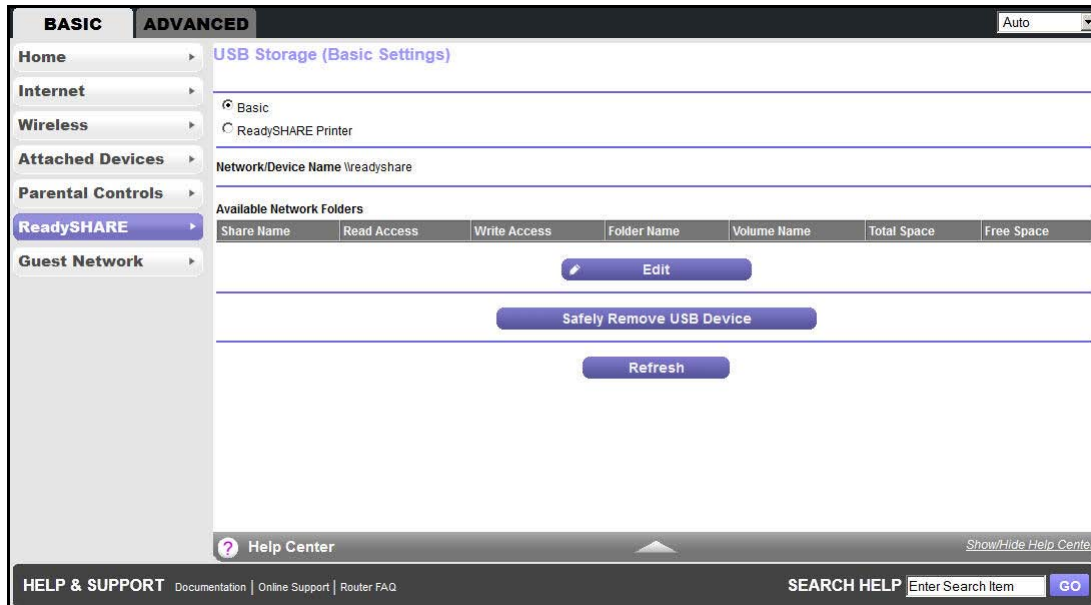
This screen displays the following when Basic is selected:

- **Network/Device Name**. The default is \\readyshare. This name is the name used to access the USB device connected to the WiFi modem router.

- **Available Network Folders**. The folders on the USB device.

   Share Name. If only one device is connected, the default share name is USB_Storage. You can click the name shown, 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 user name (account name) for All – no password is guest. The password for admin is the same one that you use to log in to the WiFi modem router. By default, it is **password**.

   Folder Name. Full path used by 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.

- **Edit**. Click the **Edit** button to edit the Available Network Folders settings.
- **Safely Remove a USB Device**. Click to safely remove the USB device attached to your WiFi modem router.

You can click **Refresh** to update this screen.

For more information about USB storage, see *Chapter 5, USB Storage*.

ReadySHARE Printer

From the BASIC Home screen, select **ReadySHARE**, and from the USB Storage (Basic Settings) screen, select **ReadySHARE Printer** to display the following screen:
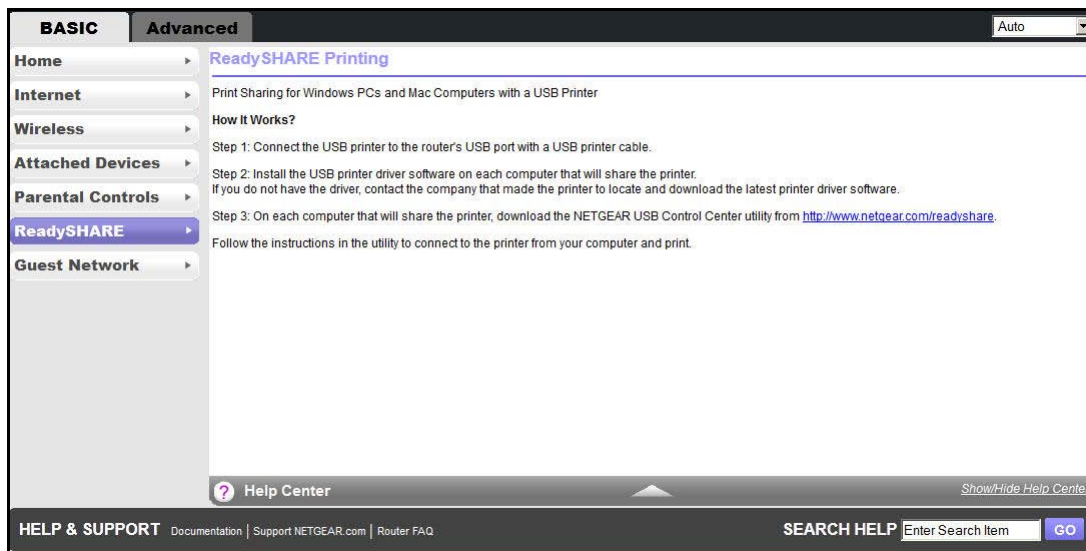
For more information about USB printing, see *Chapter 6, USB Printer Control*.

Basic Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network setup.

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

> **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 wireless network name (SSID) or other wireless security settings, you are disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the WiFi modem router.

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

1. On the Basic Home screen, select **Wireless** to display the Wireless Settings screen.

The screen sections, settings, and procedures are explained in the following sections.

2. Make any necessary changes, and click **Apply** to save your settings.

3. 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 show up on the Attached Devices screen? If it does, then it is connected to the network.

   • If you are not sure what the network name (SSID) or password is, look on the label on the bottom of your WiFi modem router.

Wireless Settings Screen Fields

Region. The location where the WiFi modem router is used. Select from the countries in the list. In the United States, the region is fixed to United States and is not changeable.

Wireless Network

> **Note:** These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and **_NETGEAR strongly recommends that you do not change this setting_**.

Channel. This setting is the wireless channel used by the gateway. Enter 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 (when indicated by lost connections or slow data transfers). If this interference happens, experiment with different channels to see which is the best.

Mode. Up to 130 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. The 300 Mbps setting allows 802.11n devices to connect at this speed.

Enable SSID Broadcast. This setting allows the WiFi modem 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. To turn off the SSID broadcast, clear the **Enable SSID Broadcast** check box and click Apply.

Enable Wireless Isolation. If this check box is selected, 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.

Security Options Settings

> **Note:** These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

The Security Options section of the Wireless Setup screen lets you change the security option and password. **_NETGEAR recommends that you do not change the security option or passphrase,_** but if you want to change these settings, this section explains how. **_Do not disable security_**.

Change WPA Security Option and Passphrase

> **Note:** These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

1. Under Security Options, select the WPA option you want.

2. In the Passphrase field that displays when you select a WPA security option, enter the network key (passphrase) that you want to use. It is a text string from 8 to 63 characters.

Guest Networks

Adding a guest network allows visitors at your home to use the Internet without using your wireless security key. You can add a guest network to each wireless network: 2.4 GHz b/g/n and 5.0 GHz a/n

➢ **To set up a guest network:**

1. From the BASIC Home screen, select **Guest Network** to display the following screen:

2. Select any of the following wireless settings:

Note: These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

Enable Guest Network. When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.

Enable SSID Broadcast. If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.

Allow guest to access My Local Network. If this check box is selected, any user who connects to this SSID has access to your local network, not just Internet access.

Enable Wireless Isolation. If this check box is selected, 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.

3. Give the guest network a name.

   The guest network name is case-sensitive and can be up to 32 characters. You then manually configure the wireless devices in your network to use the guest network name in addition to the main nonguest SSID.

4. Select a security option from the list. The security options are described in *Guest Network Wireless Security Options* on page 39.

5. Click **Apply** to save your selections.

Guest Network Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network.

This section presents an overview of the security options and provides guidance on when to use which option. It is also possible to set up a guest network without wireless security. NETGEAR does *not* recommend using no security on a wireless network.

Wi-Fi Protected Access (WPA) encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means that the product is authorized by the Wi-Fi Alliance (*http://www.wi-fi.org/*) because it complies with the worldwide single standard for high-speed wireless local area networking.

WPA-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption, implements most of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards, but not all wireless access points. It is superseded by WPA2-PSK.

WPA2-PSK is stronger than WPA. It is advertised to be indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is implemented through hardware, while WPA-PSK is implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.

WPS-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. The product documentation for your wireless adapter and WPA client software should have instructions about configuring their WPA settings.

NETGEAR genie App

The genie app is your home network dashboard. It lets you easily view, manage, and control your entire home network, and helps you fix common network problems. You can use the genie app or the genie mobile app.

genie app

Visit the NETGEAR genie web page at *www.netgear.com/genie*.

From the genie app, you can select the following:

- **Internet**. Monitor and repair Internet connectivity issues, for both wired and wireless connections.

- **WiFi Connection**. View or change your router wireless settings.

- **Router Settings**. Log in to your router to view or change its settings.

- **Network Map**. View the devices connected to your network.

- **Parental Controls**. Manage parental controls to protect devices in your network from inappropriate contents.

- **ReadySHARE**. If you connected a USB storage device or printer to the USB port on the router, then you can access its contents.

- **Support**. Support FAQs are available on your computer without an Internet connection. You can get answers to common router issues here. Some simple network tools are available to help you debug the network as well.

NETGEAR genie Mobile App

➢ **To install the genie mobile app:**

1. Using your mobile device, navigate to the Apple AppStore or Google Play for Android, and search for NETGEAR genie. You can use the following QR codes to speed up this process:

iPad app   **iPhone app**   **Android app**

2. Install the app on your iPad or phone.

3. Launch the app, and it displays the dashboard screen.
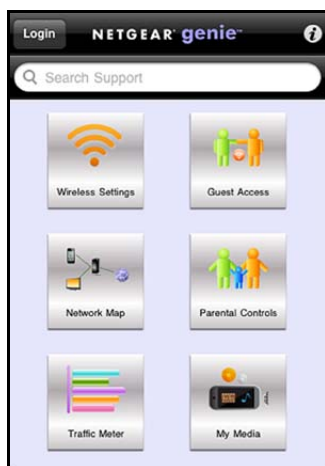
To use this app, you need a Wi-Fi connection from your phone or iPad to your NETGEAR home network.

- Manage Wi-Fi settings and guest access for your home network.
- View a map of your network.
- Set up or manage Parental Controls.
- Use the traffic meter to check your Internet usage.
- With My Media, play media on devices on your network.

NETGEAR genie ADVANCED Home

4

Specify custom settings

The ADVANCED screens are for advanced users who want to specify custom settings.

This chapter explains the features available from the NETGEAR genie ADVANCED Home screen, shown in the following figure:

This screen is also displayed through the Administration menu.
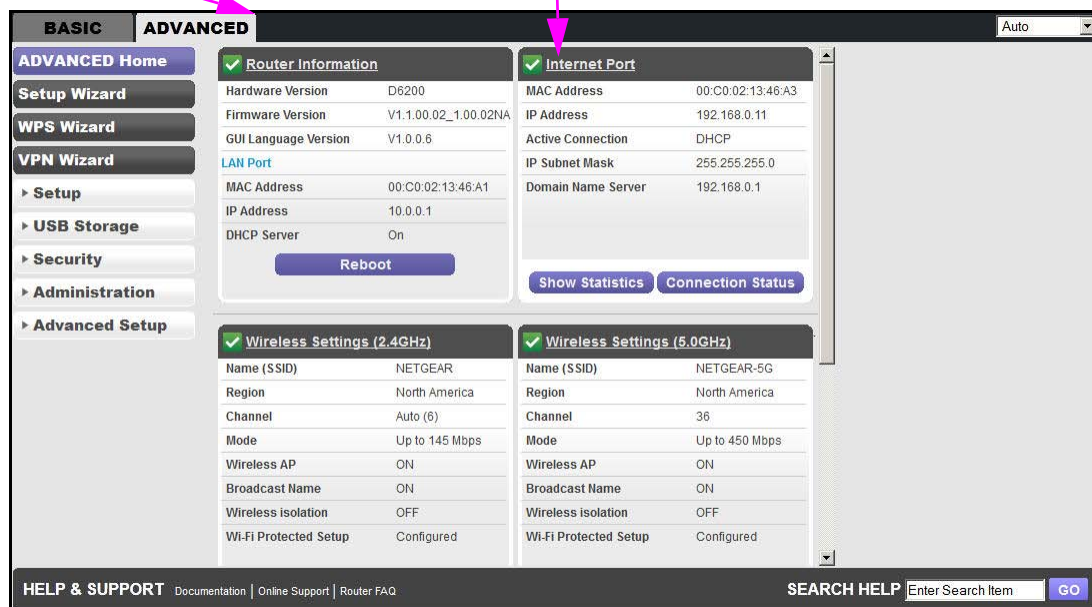
This chapter contains the following sections:

- *Setup Wizard*
- *WPS Wizard*
- *VPN Wizard*
- *Setup Menu*
- *ADSL Setup*
- *WAN Setup*
- *LAN Setup*
- *Quality of Service Setup*

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

- **USB Storage**. See *Chapter 5, USB Storage*.
- **Security**. See *Chapter 7, Security*.
- **Administration**. See *Chapter 8, Administration*.
- **Advanced Setup**. See *Chapter 9, Advanced Settings*.

Setup Wizard

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

1. Select **Setup Wizard** to display the following screen:
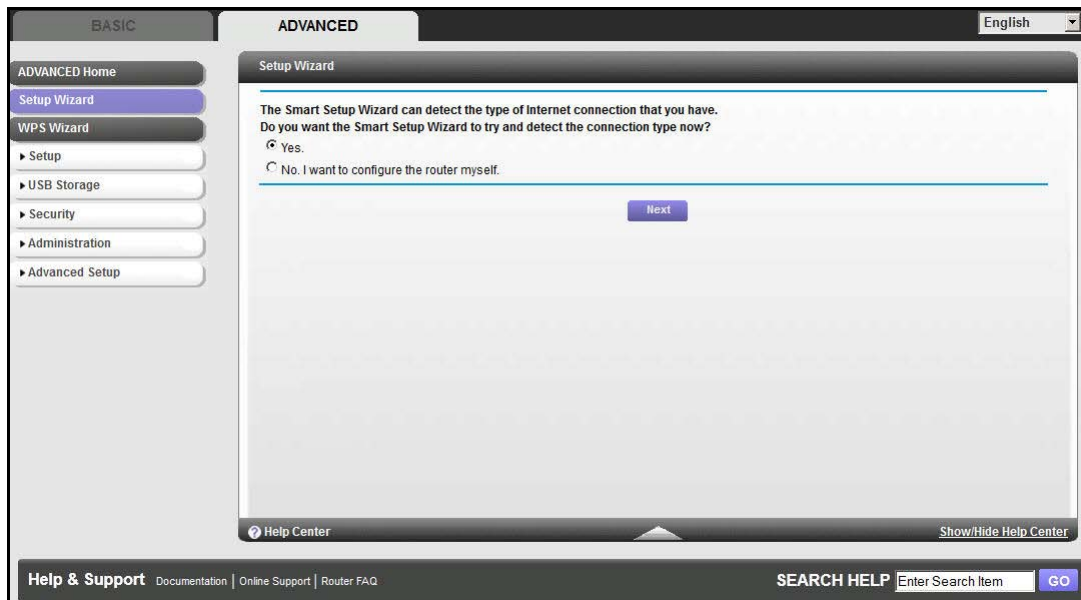
2. Select either **Yes** or **No, I want to configure the router myself**. If you select No, you are taken to the Internet Basic Settings screen (see *Internet Basic Settings* on page 30).

3. If you selected Yes, click **Next**. A series of screens are displayed as the router discovers and processes your Internet connection. Click **Next** when prompted to advance to the next screen.

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

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 have to either press its WPS button or locate its WPS PIN.

➢ **To use the WPS Wizard:**

1. Select **ADVANCED > WPS Wizard**. The following screen displays:
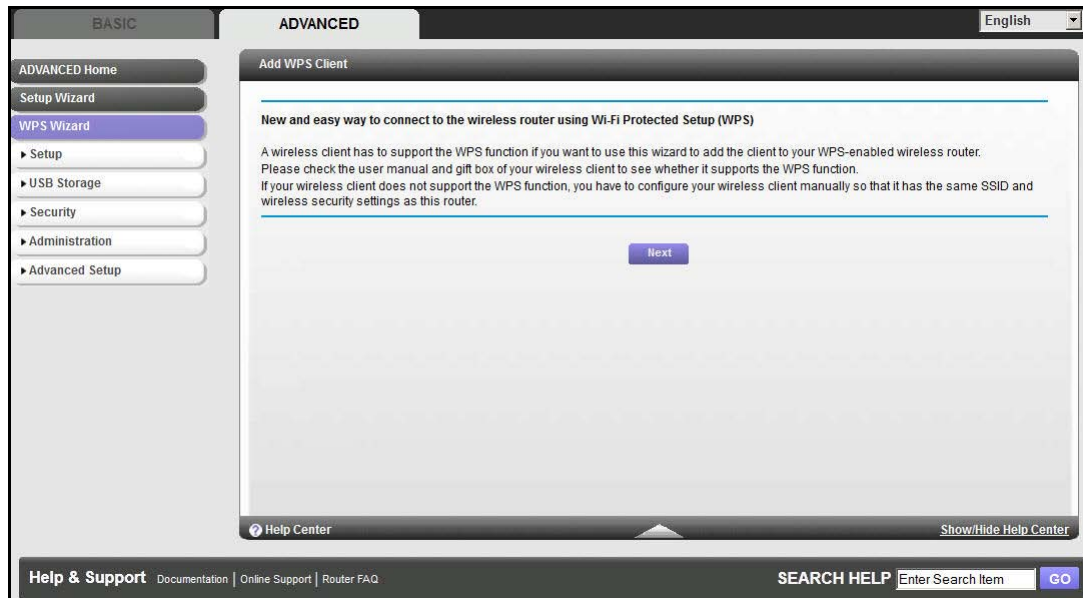
2. Click **Next**. The following screen lets you select the method for adding the WPS client (a wireless device or computer).
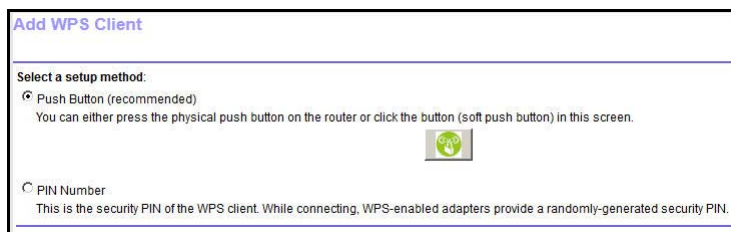
You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.

   • To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button on the top of the WiFi modem router. Within 2 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 **Next**.

Within 2 minutes, go to the client device and use its WPS software to join the network without entering a password.

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

4. Repeat Step 2 and Step 3 to add another WPS client to your network.

VPN Wizard

The Wizard asks you series of questions that determine the IPSec keys and VPN policies it sets up. The VPN Wizard sets the parameters for the network connection, Security Association, traffic selectors, authentication algorithm, and encryption. These parameters are based on the VPNC recommendations. More information about the VPNC recommendations is presented in the VPN Wizard summary page.

➢ **To use the VPN Wizard:**

1. Select **ADVANCED > VPN Wizard**. The following screen displays:
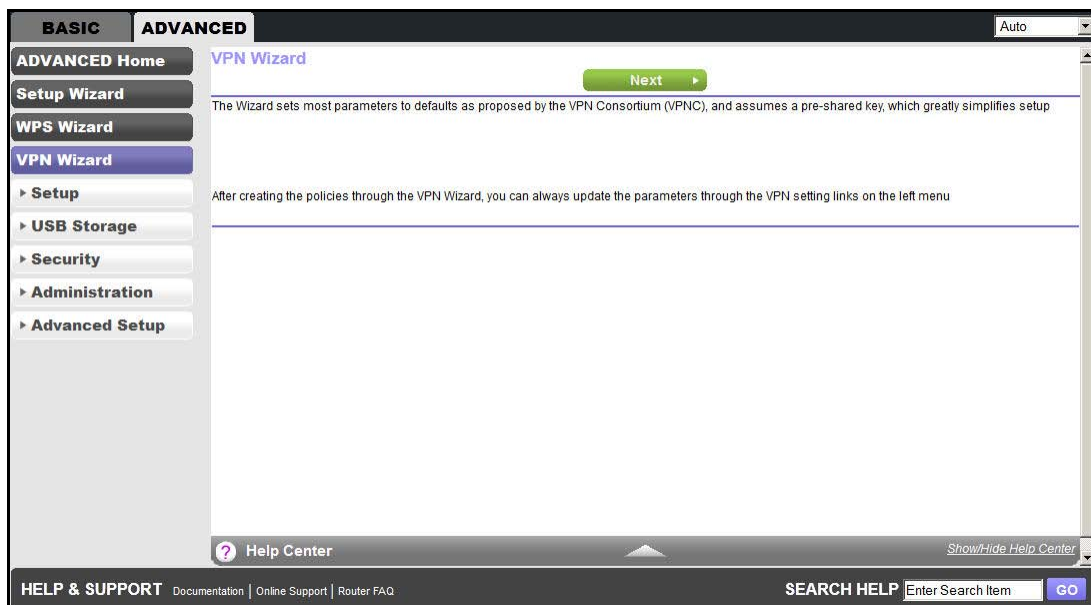
2. Click **Next**. The following screen displays:

Enter the requested information:

- **Connection name**. Enter an appropriate name for the connection. This name is not supplied to the remote VPN endpoint. Rather, it is used to help you manage the VPN settings.

- **Pre-shared key**. The key has to be entered both here and on the remote VPN Gateway or the remote VPN client. This method does not require using a CA (Certificate Authority).

- **VPN tunnel connection**. The wizard has to know if you are planning to connect to a remote gateway or setting up the connection for a remote client or computer to establish a secure connection to this device.

3. Click **Next**. The following screen displays:

Enter the remote IP address of the gateway you want to connect to, or provide the Internet name of the gateway. The Internet name is the fully qualified domain name, as set up in a Dynamic DNS service.

4. Click **Next**. The following screen displays:

Enter the remote LAN IP address and subnet mask of the remote gateway.

- If this information does not match the LAN IP address and subnet mask in the remote gateway, the secure tunnel fails to connect.

- The IP address range used on the remote LAN has to be different from the IP address range used on the local LAN.

5. Click **Next**. The following screen displays:

This screen shows the summary of the Wizard configuration with a link to view the VPNC recommended parameters (click **here** to view the VPNC-recommended parameters).

6. Click **Done**. The following screen displays:

7. For information about how to add or modify VPN policies, see *VPN Policies* on page 123.

Setup Menu

Select **ADVANCED > Setup** to display the Setup menu. The following selections are available:

- **Internet Setup**. This selection is a shortcut to the same Internet Basic Settings screen that you can access from the dashboard on the BASIC Home screen. See *Internet Basic Settings* on page 30.

- **ADSL Setup**. Internet (ADSL) setup. See *ADSL Setup* on page 49.

- **Wireless Setup**. This selection 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 35.

- **WAN Setup**. Internet (WAN) setup. See *WAN Setup* on page 50.

- **LAN Setup**. Local area network (LAN) setup. See *LAN Setup* on page 53.

- **QoS Setup**. Quality of Service (QoS) setup. See *Quality of Service Setup* on page 56.

- **Guest Network**. This selection is a shortcut to the same Wireless Settings (for guest networks) screen that you can access from the dashboard on the BASIC Home screen. See *Guest Networks* on page 38.

ADSL Setup

The ADSL Settings screen lets you configure the multiplexing method and virtual circuit of your ADSL connection. The default parameters should be correct to match the system used by your ISP. Select **ADVANCED > Setup > ADSL Settings** to dispay the following screen:

- **Multiplexing Method**. Your ISP indicates whether your multiplexing method is VC-BASED or LLC-BASED.
- **VPI**, **VCI**. Your ISP indicates which VPI and VCI combination is used for your service.
- **DSL Mode**. Your ISP indicates that the best setting is used for your DSL connection.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the WiFi modem router to respond to a ping on the WAN (Internet) port. Select **ADVANCED > Setup > WAN Setup** to view the following screen:
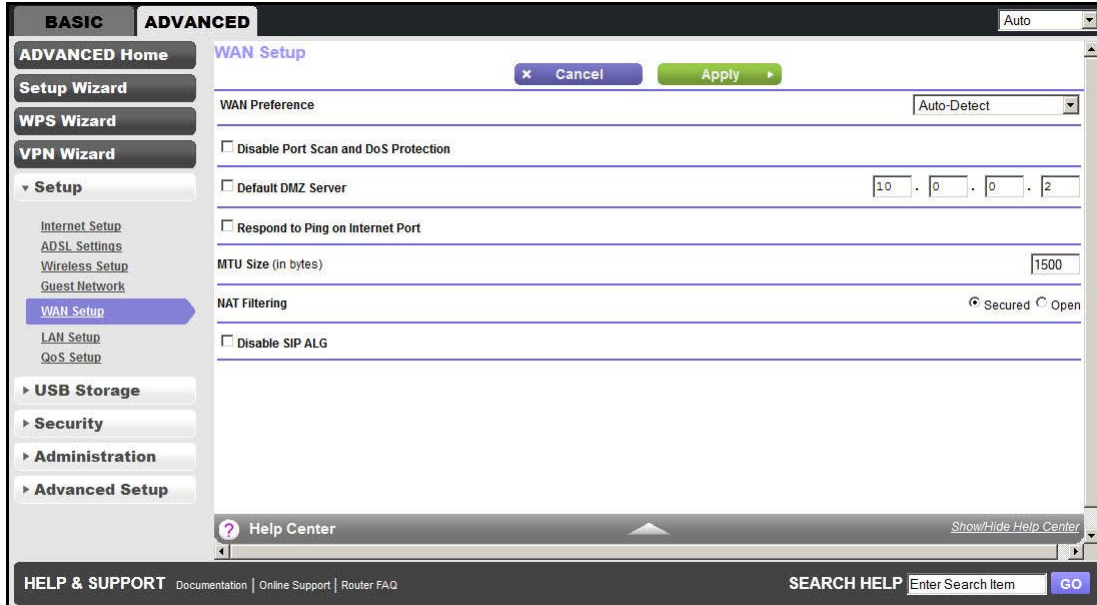
- **WAN Preference**. Select your WAN preference: Auto Detect, Must use DSL WAN, or Must use Ethernet WAN.

- **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 feature should be disabled 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. See the following section, *Default DMZ Server*, for more details.

- **Respond to Ping on Internet Port**. If you want the WiFi modem router to respond to a ping from the Internet, select this check box. Use this setting only as a diagnostic tool because it allows your WiFi modem 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 change 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 51.

- **Disable IGMP Proxying**. The IGMP Proxying function lets a LAN computer receive the multicast traffic it is interested in from the Internet. Click this check box to disable the function if you do not need it.

- **NAT Filtering**. Network Address Translation (NAT) determines how the WiFi modem 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. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function.

- **Disable SIP ALG**. Some VoIP applications do not work well with the SIP ALG. Enabling this option to turn off the SIP ALG might help your VoIP devices to create or accept a call through the router.

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 WiFi modem 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 is discarded by the WiFi modem 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. On the WAN Setup screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. 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 have to 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 8. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR WiFi modem routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not 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. Select **ADVANCED > Setup > WAN Setup**.
2. In the MTU Size field, enter a new size from 64 through 1500.
3. Click **Apply** to save the settings.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

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

- LAN IP address. **192.168.0.1**
- 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 a different IP addressing scheme, make changes in the LAN Setup screen.

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

> ➤ **To change the LAN settings:**

1. Select **ADVANCED > Setup > LAN Setup** to display the following screen:
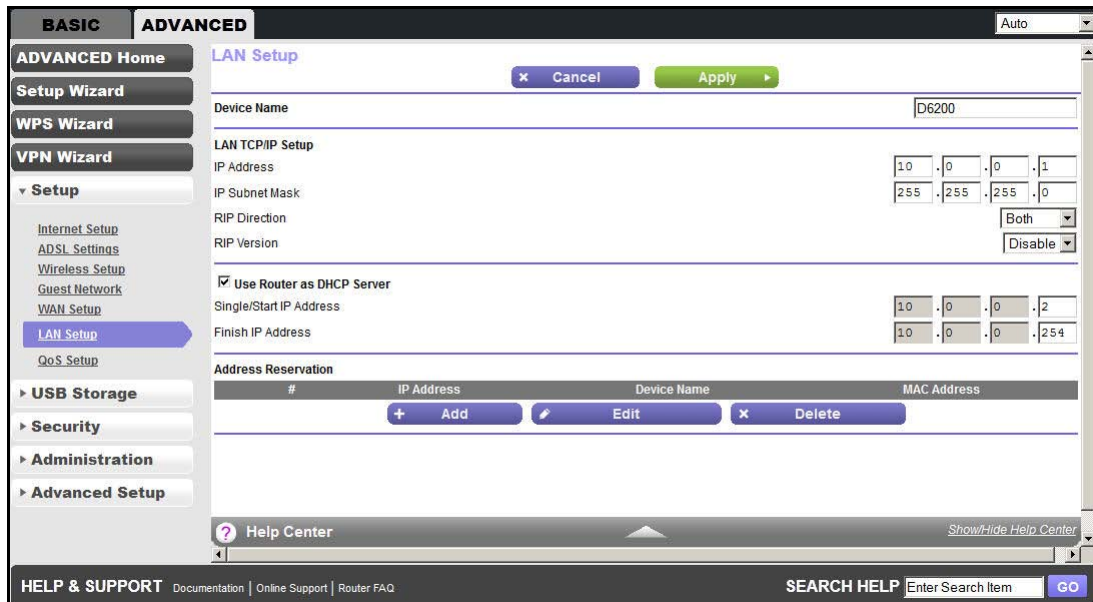
2. Enter the settings that you want to customize. These settings are described in the following section, *LAN Setup Screen Settings*.

3. Click **Apply** to save your changes.

LAN Setup Screen Settings

LAN TCP/IP Setup

- **IP Address**. The LAN IP address of the WiFi modem router.

- **IP Subnet Mask**. The LAN subnet mask of the WiFi modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or WiFi modem router.

- **RIP Direction**. Router Information Protocol (RIP) allows 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 WiFi modem router sends. It recognizes both formats when receiving. By default, the RIP function is disabled.
    - **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.

Use Router as a DHCP Server

This check box is selected so that the WiFi modem router functions as a Dynamic Host Configuration Protocol (DHCP) server.

- **Starting IP Address**. Specify the start of the range for the pool of IP addresses in the same subnet as the WiFi modem router.

- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the WiFi modem router.

Address Reservation

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

Use the WiFi Modem Router as a DHCP Server

By default, the WiFi modem router functions as a DHCP server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the WiFi modem

router's LAN. The assigned default gateway address is the LAN address of the WiFi modem router. The WiFi modem 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 WiFi modem router are satisfactory.

You can specify the pool of IP addresses that are assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the WiFi modem router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

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

- An IP address from the range you defined
- Subnet mask
- Gateway IP address (the WiFi modem router's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Internet Basic Settings screen; otherwise, the WiFi modem router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Internet Basic Settings screen)

To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, you need to set your computers' IP addresses manually or they are not able to access the WiFi modem 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 WiFi modem 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. In the Address Reservation section of the screen, click the **Add** button. The following screen displays:

2. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the WiFi modem router's LAN subnet, such as 192.168.0.x.)

3. 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.

4. Click **Apply** to enter the reserved address into the table.

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

To edit or delete a reserved address entry, select the radio button next to the reserved
address you want to edit or delete. Then click **Edit** or **Delete**.

Quality of Service Setup

Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of
traffic ahead of others. The WiFi Modem Router can provide QoS prioritization over the
wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen.

Select **ADVANCED > Setup > QoS Setup** to display the following screen:
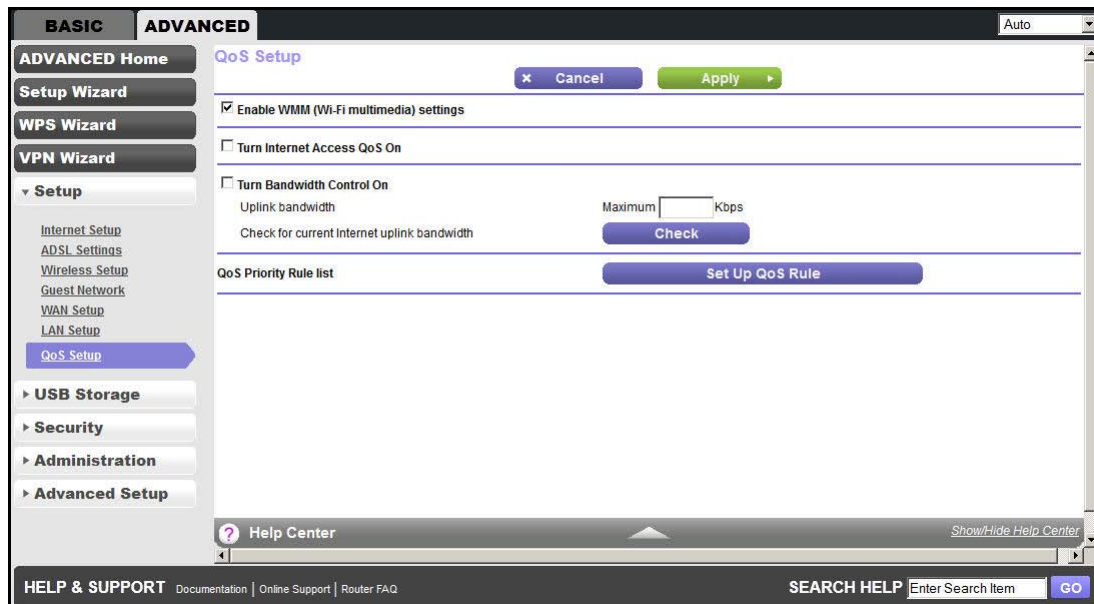
Enable WMM QoS for Wireless Multimedia Applications

The WiFi Modem Router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to
prioritize wireless voice and video traffic over the wireless link. WMM QoS provides
prioritization of 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 the application and the client running that application must 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. You can disable it in the QoS Setup screen by clearing the **Enable WMM** check box and clicking **Apply**.

Set Up QoS for 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 WiFi modem router
- A specific device by MAC address

To specify prioritization of traffic, you have 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.

QoS for Applications and Online Gaming

➢ **To create a QoS policy for applications and online games:**

1. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.

2. Click the **Setup QoS Rule** button to see the existing priority rules. On this screen, you can edit or delete a rule by selecting its radio button and clicking either the **Edit** or **Delete** button. To delete all of the rules, click the **Delete All** button.

QoS Priority Rule list

	#	QoS Policy	Priority	Description
○	1	MSN Messenger	High	MSN Messenger application
○	2	Yahoo Messenger	High	Yahoo Messenger application
○	3	IP Phone	Highest	IP Phone application
○	4	Vonage IP Phone	Highest	Vonage IP Phone application
○	5	NetMeeting	High	NetMeeting application
○	6	AIM	High	AIM application
○	7	Google Talk	Highest	Google Talk application
○	8	Netgear EVA	Highest	Netgear EVA application
○	9	Counter Strike	High	On-line gaming Counter Strike
○	10	Age of Empires	High	On-line gaming Age of Empires
○	11	Everquest	High	On-line gaming Everquest
○	12	Quake 2	High	On-line gaming Quake 2
○	13	Quake 3	High	On-line gaming Quake 3
○	14	Unreal Tournament	High	On-line gaming Unreal Tournament
○	15	Warcraft	High	On-line gaming Warcraft

3. To add a priority rule, scroll down to the bottom of the QoS Setup screen and click **Add Priority Rule** to display the following screen:

4. In the QoS Policy for field, type the name of the application or game.

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

In either case, a list of applications or games displays in the list.

6. In the Applications list, you can select an existing item, or you can scroll and select **Add a New Application** or **Add a New Game,** as applicable.

    a. When you add an entry, the QoS - Priority Rules screen expands as shown:

    b. In the QoS Policy for field, enter a descriptive name for the new application or game.

    c. In the Connection Type list, select either **TCP, UDP,** or both (**TCP/UDP**), and specify the port number or range of port numbers used by the 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. The options are Low, Normal, High, and Highest.

8. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

QoS for a WiFi Modem Router LAN Port

➢ **To create a QoS policy for a device connected to one of the WiFi modem router's LAN ports:**

1. Select **ADVANCED > Setup > QoS Setup** to display the QoS Setup screen. Select the **Turn Internet Access QoS On** check box.

2. Click the **Setup QoS Rule** button.

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

4. From the Priority Category list, select **Ethernet LAN Port**, as shown in the following figure:

5. From the LAN port list, select the LAN port that has a QoS policy.

6. From the Priority list, select the priority that this port's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.

7. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

8. In the QoS Setup screen, click **Apply**.

QoS for a MAC Address

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

1. Select **ADVANCED > Setup > QoS Setup**, and click the **Setup QoS Rule** button. The QoS Setup screen displays.

2. Click **Add Priority Rule**.

3. From the Priority Category list, select **MAC Address** to display the following screen:

4. From the Priority list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest. Click **Add** to add this rule to MAC Device List.

5. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

6. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.

7. Click **Apply**.

Edit or Delete an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

1. Select **ADVANCED > QoS Setup** to display the QoS Setup screen.

2. Select the radio button next to the QoS policy to be edited or deleted, and do one of the following:

    •   Click **Delete** to remove the QoS policy.

    •   Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.

3. Click **Apply** in the QoS Setup screen to save your changes.

USB Storage

5

Access and configure a USB storage drive

This chapter describes how to access and configure a USB storage drive attached to your WiFi modem router. The USB port on the WiFi modem router can connect only to USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, printers, CD drives, or DVD drives to the WiFi modem router USB port.
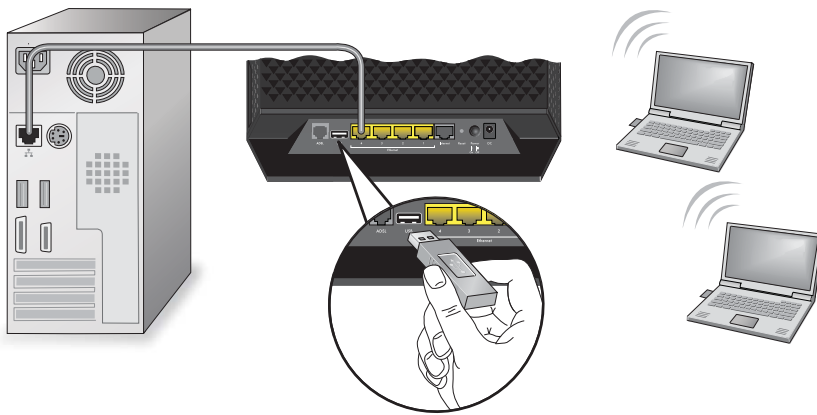
This chapter contains the following sections:

- *USB Drive Requirements*
- *ReadySHARE Access*
- *File-Sharing Scenarios*
- *USB Storage Basic Settings*
- *USB Storage Advanced Settings*
- *Safely Remove a USB Drive*
- *Media Server Settings*
- *Specify Approved USB Devices*
- *Connect to the USB Drive from a Remote Computer*

USB Drive Requirements

The WiFi modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown in the following table. Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables.

Table 9. USB drive speeds

Bus	Speed/Sec
USB 1.1	12 Mbits
USB 2.0	480 Mbits

The WiFi modem router should work with most USB-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the WiFi modem router, visit:

http://kbserver.netgear.com/readyshare

The WiFi modem router supports both read and write access for FAT16, FAT32, NTFS, and Linux file systems (EXT2 and EXT3).

Note: Some USB external hard drives and flash drives require drivers to be loaded into the computer before the computer can access the USB device. Such USB devices do not work with the WiFi modem router.

ReadySHARE Access

Once you have set up your WiFi modem router, you can connect any USB storage device and share the contents with other users on your network.

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

- On Windows 7, Windows XP, Windows Vista, and Windows 2000 systems, select **Start > Run** and enter **\\readyshare** in the dialog box. Click **OK**.
- On Windows 7, Windows XP, Windows Vista, and Windows 2000 systems, open either 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.

File-Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any Windows, Mac, or Linux file type including text, Word, PowerPoint, Excel, and MP3 files, pictures, and multimedia. USB drive applications include:

- Sharing multimedia such as MP3 files, pictures, and other multimedia with local and remote users.

- Sharing resources on your network. You might want to 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 files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Share Photos

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

➢ **To share files with your friends and family:**

1. Insert your USB drive into the USB port on the WiFi modem 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 *USB Storage Advanced Settings* on page 67.

Store Files in a Central Location for Printing

This scenario is for a family that has one high-quality color printer directly attached to a computer, but not shared on the local area network (LAN). This family does not have a print server.

- One family member has photos on a Macintosh computer that she wants to print.

- The photo-capable color printer is directly attached to a computer, but not shared on the network.

- The Mac and Windows computer are not visible to each other on the network.

➢ **To print photos from a Mac on the printer attached to a Windows computer:**

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 the Windows computer, use a web browser or Microsoft Networking to copy the files from the USB drive to the Windows computer. Then print the files.

Share Large Files over the Internet

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

Sharing files with a remote colleague involves the following considerations:

• There are two user accounts: admin and guest. The password for admin is the same one that you use to access the WiFi modem router. By default, it is **password**. The guest user account has no password.

• On the FTP site, the person receiving the files should use the guest user account and enter any 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 enable the HTTP (via Internet) option on the USB Storage (Advanced Settings) screen to share large files. This option supports downloading files only.

USB Storage Basic Settings

You can view or edit basic settings for the USB storage device attached to your WiFi modem router.

You can access this feature by selecting **BASIC > ReadySHARE**, or **ADVANCED > USB Storage > ReadySHARE**. The USB Storage (Basic Settings) screen displays:
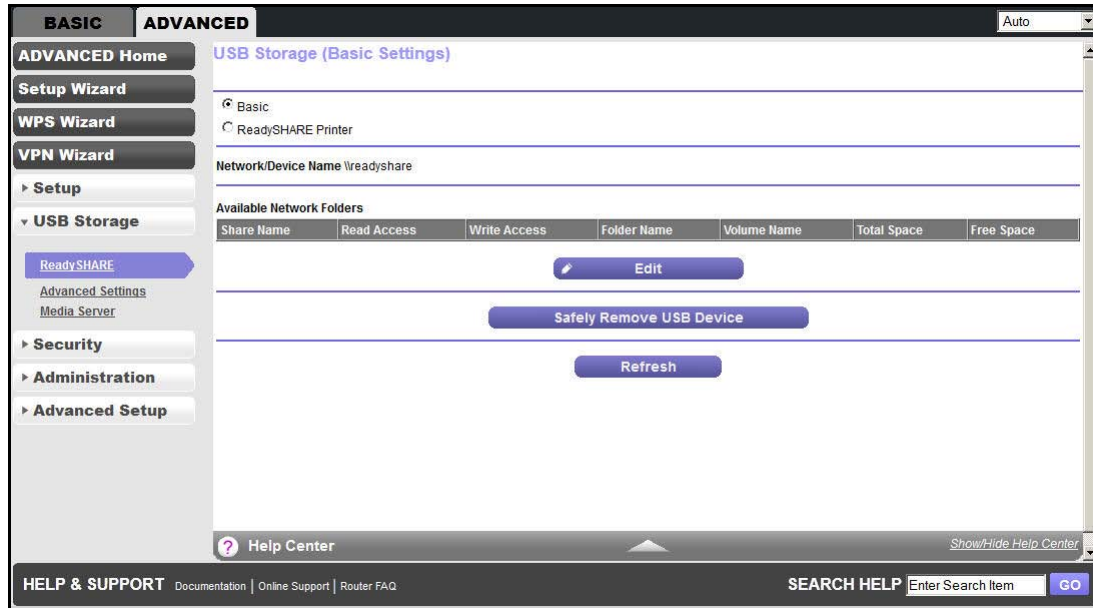
By default, the USB storage device is available to all computers on your local area network (LAN).

➢ **To access your USB device:**

1. Click the network device name or the share name in your computer's network folders list.

2. For SMB://readyshare, click **Connect**.

Note: If you logged in to the WiFi modem router before you connected your USB device, you might not see your USB device in the WiFi modem router screens until you log out and then log back in again.

Add or Edit a Network Folder

1. You can access this feature by selecting **BASIC > ReadyShare > Edit**, or **ADVANCED > USB Storage > Advanced Settings**.
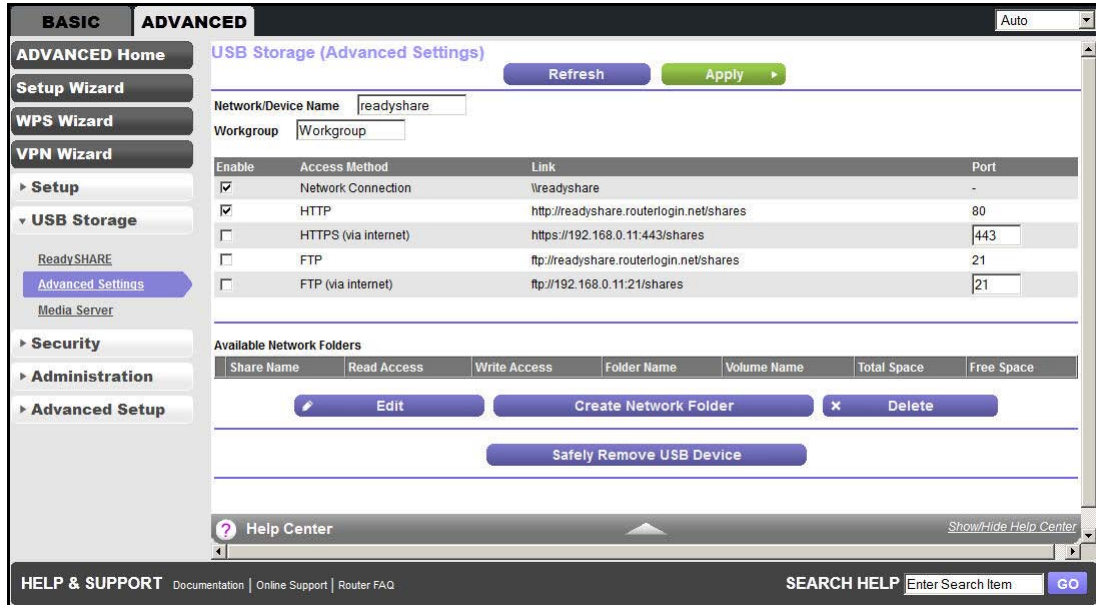
2. Specify the changes that you want to make:
   • To add a folder, click **Create Network Folder**.
   • To edit a folder, select its radio button and click **Edit**.

3. You can use this screen to select a folder, to change the share name, or to change the read access or write access from All - no password to **admin**.

   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 WiFi modem router. By default, it is password.

4. Click **Apply** for your changes to take effect.

USB Storage Advanced Settings

You can set up the device name, workgroups, and network folders for your USB device. On the Advanced tab, select **USB Storage > Advanced Settings** to display the following screen:
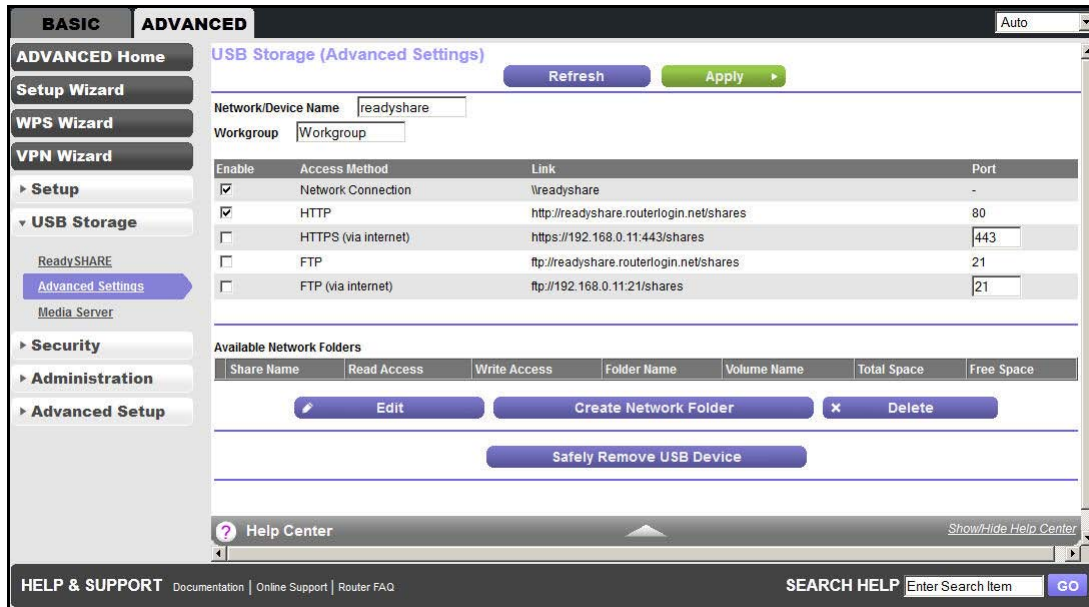
You can use this screen to specify access to the USB storage device.

- **Network Device Name**. The default is ReadySHARE. This name is used to access the USB device connected to the WiFi modem router.

- **Workgroup**. If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows.

- **Access Method**. The access methods are described here.

  - **Network Connection**. Enabled by default, this connection allows all users on the LAN to have access to the USB drive.

  - **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 setting, 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 setting supports file uploading only.

  - **FTP**. Disabled by default.

  - **FTP (via internet)**. Disabled by default. If you enable this setting, remote users can access the USB drive through FTP over the Internet. This setting supports both downloading and uploading of files.

Available Network Folders

You might need to scroll down to view this section of the screen:

- **Share Name**. If only one device is connected, the default share name is USB_Storage. You can click the name shown, 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 WiFi modem router.

- **Folder Name**. Full path used by 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.

Safely Remove a USB Drive

To safely remove a USB disk drive so that no users can access it, select **USB Storage > Basic Settings**, or **ADVANCED > USB Storage > Advanced Settings**, and click the **Safely Remove USB Device** button. This procedure takes the drive offline.

Media Server Settings

By default, the WiFi modem router is set up to act as a ReadyDLNA media server, which lets you view movies and photos on DLNA/UPnP AV–compliant media players, such as Xbox360, Playstation, and NETGEAR's Digital Entertainer Live.

To view these settings, select **ADVANCED > USB Storage > Media Server** to display the following screen:
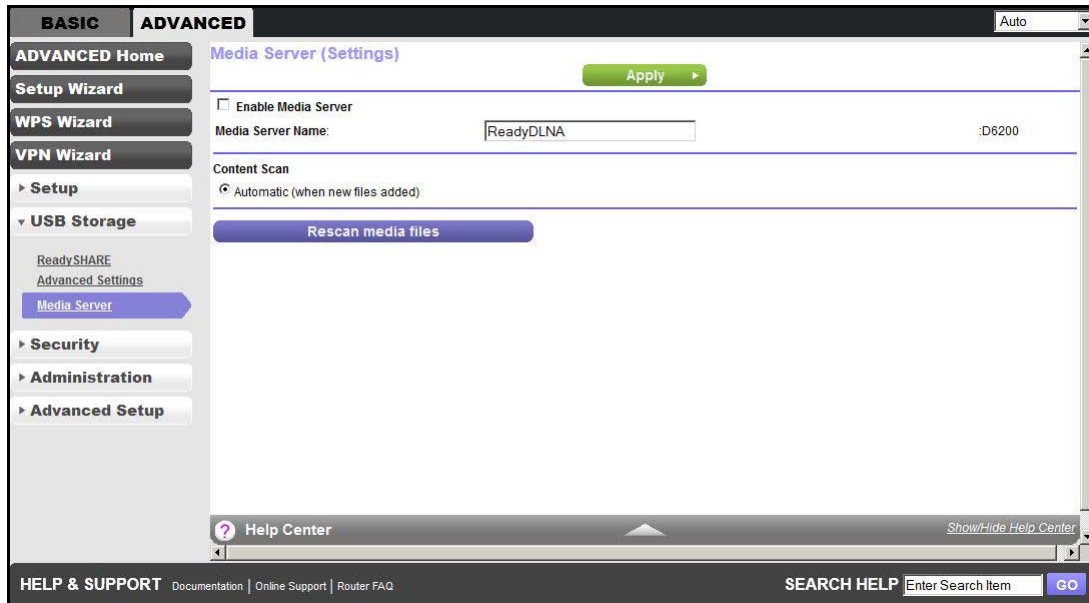
By default the Enable Media Server check box and the Automatic (when new files are added) radio button are selected. When these options are selected, the WiFi modem router scans for media files whenever new files are added to the ReadySHARE USB hard drive.

Specify Approved USB Devices

For more security, you can set up the WiFi modem router to share approved USB devices only. You can access this feature from the Advanced Setup menu on the Advanced tab.

➢ **To set up approved USB devices:**

1. Select **ADVANCED > Advanced Setup > USB Settings**. The following screen displays:

2. Click the **Approved Devices** button. The USB Drive Approved Devices screen displays:

This screen shows the approved USB devices and the available USB devices. You can remove or add approved USB devices.

3. To add an approved USB device, select it from the Available USB Devices list and click **Add**.

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

5. Click **Apply** so that your change takes effect.

If you want to work with another USB device, you have to click the **Safely Remove USB Device** button for the currently connected USB device. Connect the other USB device and repeat this process.

Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers with a web browser, you have to use the WiFi modem 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 WiFi modem router's Internet IP address from the dashboard on the BASIC Home screen or the ADVANCED Home screen.

Access the WiFi Modem Router USB Drive Remotely Using FTP

➢ **To connect to the WiFi modem router's USB drive using a web browser:**

1. Connect to the WiFi modem router by typing **ftp://** and the Internet port IP address in the address field of Internet Explorer or Netscape Navigator, for example:

    ftp://10.1.65.4

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

2. 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**.

3. The directories of the USB drive that your account can access are displayed, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

USB Printer Control

Access and configure a USB printer

6

This chapter describes how to access and configure a USB printer attached to your WiFi modem router.
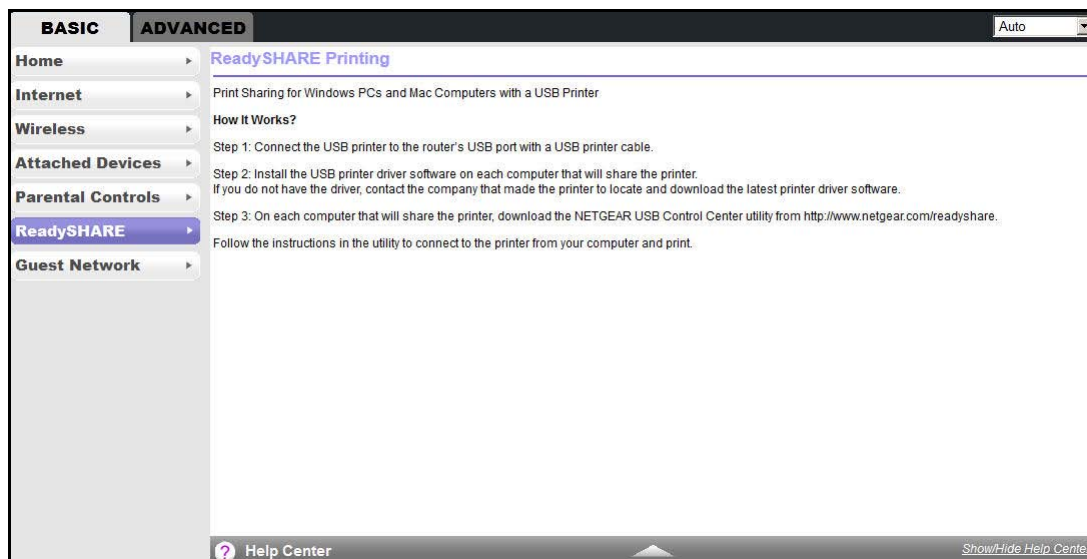
The USB Control Center utility allows you to control a shared USB device such as a printer from your computer that is connected to the USB port on your router.

The utility has to be installed on each computer on your network from which you want to control the device. You can download this utility at *www.netgear.com/landing/en-us/readyshare.aspx*.

When you launch the USB Control Center Utility, a screen similar to the following displays:
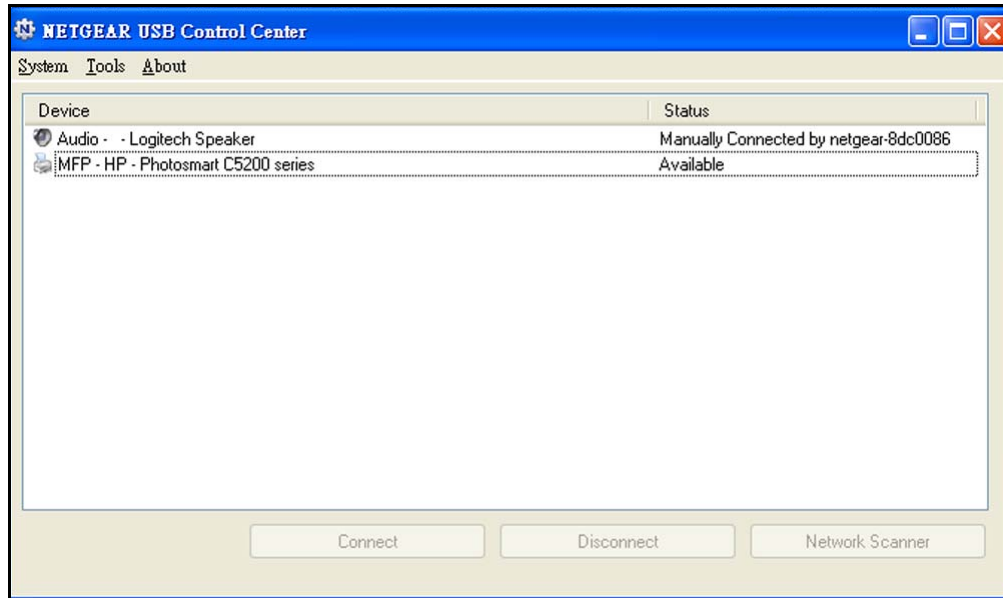
This screen is the main screen, which shows a device icon, the description for this USB device, and its status.

- **Available**. The device is available from the computer that you are using.
- **Waiting to Connect**. You need to connect to this device from the computer that you are using. If you are connecting for the first time, you might be prompted to install the device driver.

The following menu selections are available:

- **System**. Exit the utility.
- **Tools**. Access the Control Center Configuration to set up your shared USB device. See the following section, *Control Center Configuration*.
- **About**. View details about the USB Control Center software.

This chapter includes the following sections:

- *Control Center Configuration*
- *USB Printer*
- *Scan with a Multifunction Printer*

Control Center Configuration

Select **Tools > Configuration** to display the following screen:

Automatically execute when logging on Windows. Select this check box to have the utility start automatically when you are logged in to Windows.

Timeout. Specify the time-out value for holding the USB resource when it is not in use.

Language. Select the display language for this utility.

USB Printer

The first time you use a printer, you need to click **Connect**. You might be asked to install the driver for this printer. After the driver is installed, the printer status changes to Available.

> **Note:** Some USB printers (for example, HP and Lexmark printer) request that you do not connect the USB cable until the installation software prompts you.

If the USB printer is detected and connected automatically, you need to disconnect the printer and wait for the prompt asking you to click **Connect**.

Once the printer shows Available status, the grayed out Paused state no longer displays in the Windows Printers and Faxes window.
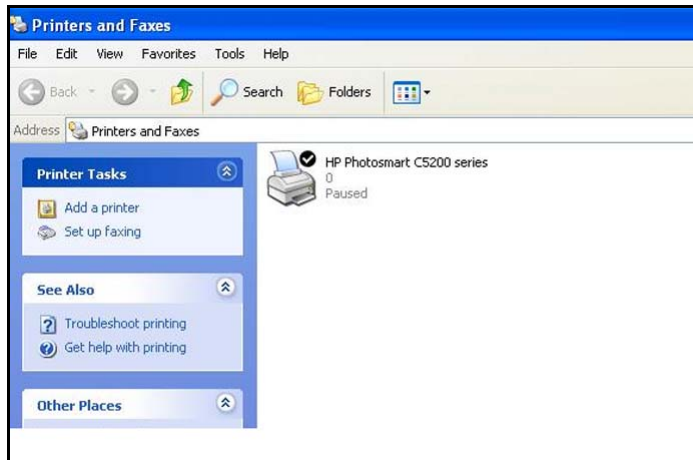
This USB printer is ready. The utility does not need to always hold the connection of this USB printer. After a print job is created for this printer, the USB utility connects to this USB printer automatically and prints. After the print job is done, the printer status returns to the Paused state.

Scan with a Multifunction Printer

You can use the scan feature of a multifunction printer.

1. Make sure that the printer's status shows as Available.
2. Click the **Network Scanner** button.

   This procedure activates the scanner window that is used to perform the scans.

Security 7
Keep unwanted content out of your network

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

This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Firewall Rules*
- *Add Custom Services to Allow or Block*
- *Schedule for Firewall Rules*
- *Security Event Email Notifications*

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.

1. Select **ADVANCED > Security > Block Sites** to display the following screen:

2. 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.

3. 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. Select the keyword you want to delete from the list.
2. Click **Delete Keyword** and then **Apply** to save your changes.

➢ **To specify a trusted computer:**

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

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply** to save your changes.

Firewall Rules

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 other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is 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." Service numbers for other applications are typically chosen from the range 1024–65535 by the authors of the application. Although the WiFi modem router already holds a list of many service port numbers, you are not limited to these choices. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

The Firewall Rules screen lets you block or allow specific Internet traffic services by computers on your network. This process is called service blocking or port filtering.

Note: This feature is for Advanced Administrators only! Incorrect configuration can cause serious problems.

➢ **To create firewall rules:**

1. Select **ADVANCED > Security > Firewall Rules** to display the following screen:

The Firewall Rules screen lists all firewall rules that have been changed from their default settings. The default rules allow all outgoing traffic and block all incoming traffic.

- To change the firewall rules for outbound traffic, you need to edit them from the Outbound Services screen as described in *Step 2*.

- To change the firewall rules for inbound traffic, you need to edit them from the Port Forwarding/Port Triggering screen as described in *Port Forwarding and Triggering* on page 103.

The Outbound Services and Inbound Services screens list the available services you can allow or block. You can also define your own custom services to allow or block with the Add Service screen as described in *Add Custom Services to Allow or Block* on page 80. Once you add your own custom services, they are available on the Outbound Services and Inbound Services screens.

You can also specify whether these services are always allowed or blocked, or allowed or blocked per schedule as described in *Schedule for Firewall Rules* on page 82.

2. **Outbound Services**. To allow or block an outbound service, click **Add** to display the following screen:

Use the Outbound Services screen to define a new outbound firewall rule, or edit an existing rule. The outbound firewall rules are used to block or allow access by computers on your network to services or applications on the Internet.

a. **Service**. Select the service or application to be covered by this rule. If the service or application you want does not appear in the list, you have to define it as described in *Add Custom Services to Allow or Block* on page 80.

b. **Action**. Select the action you want for traffic covered by this rule:
   - **BLOCK always**. Always block the traffic covered by this rule.
   - **BLOCK by schedule, otherwise Allow**. Allow the traffic covered by this rule, unless it is blocked according to the schedule specified on the Schedule screen in *Schedule for Firewall Rules* on page 82.
   - **ALLOW always**. Always allow the traffic covered by this rule (this selection is the default setting).

- **ALLOW by schedule, otherwise Block**. Block the traffic covered by this rule, unless it is blocked according to the schedule specified on the Schedule screen in *Schedule for Firewall Rules* on page 82.

  ALLOW rules are useful only when the traffic is already covered by a BLOCK rule. You would use these rules when you want to allow a subset of traffic that is blocked by another rule.

c. **LAN Users**. These settings determine which computers on your network are affected by this rule, based on their source (LAN) IP address. Select the option you want:

- **Any**. All local IP addresses are covered by this choice.
- **Address range**. You have to provide the Start and End fields when this option is selected.
- **Single address**. Enter the required address in the Start field.

d. **WAN Servers**. These settings determine which Internet locations are covered by the rule, based on their destination (WAN) IP address. Select the option you want:

- **Any**. All Internet IP addresses are covered by this choice.
- **Address range**. You have to provide the Start and End fields when this option is selected.
- **Single address**. Enter the required address in the Start field.

e. **Log**. This setting determines whether traffic covered by this rule is logged. Select the action you want:

- **Always**. This choice always logs traffic that is covered by this rule, whether it matches or not. (This feature is useful when you are debugging your rules.)
- **Never**. This choice never logs traffic covered by this rule, whether it matches or not.

f. Click **Apply** to have your changes take effect, or click **Cancel** to return to the previous screen.

3. **Inbound Services**. To allow or block an inbound service, click **here** to set up inbound firewall rules for gaming or other applications. You are redirected to the Port Forwarding/Port Triggering screen as described in *Port Forwarding and Triggering* on page 103.

4. **Instant Messaging (IM) Ports**. To close or open the instant messaging ports, select the appropriate radio button:
- Close IM Ports
- Open IM Ports (IM ports are open by default)

5. Click **Apply** to enable your Firewall Rules selections.

Add Custom Services to Allow or Block
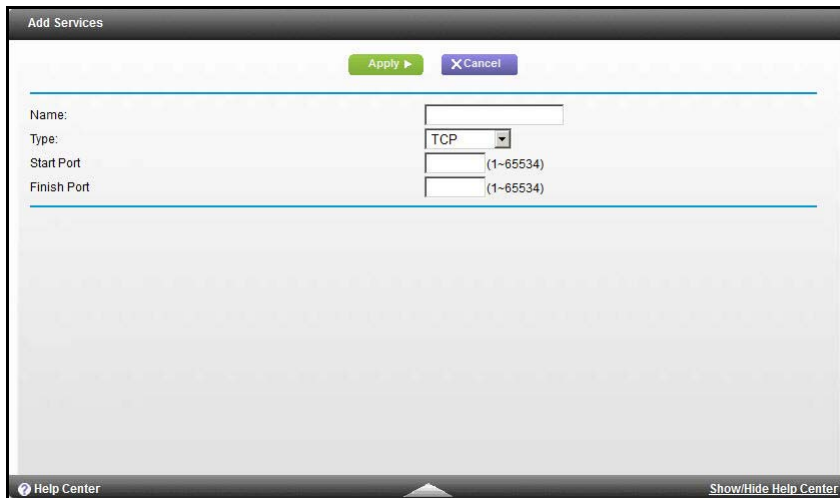
You can define your own incoming and outgoing custom services to allow or block. Once you add your own custom services, they are available on the Outbound Services screen (as

described in *Firewall Rules* on page 78) and the Inbound Services screen (as described in *Port Forwarding and Triggering* on page 103).

➢ **To add a custom service:**

1. Click **Add Custom Service** to add a service. The Add Service screen displays:

The Add Service screen allows you to specify or edit your own custom service definition. You can then use the custom service when creating firewall rules.

2. To add a service for blocking, first determine which port number or range of numbers is used by the application.

3. In the Name field, enter a suitable name for this service.

4. In the Type list, select the correct type for this service (if in doubt, select TCP/UDP):

    *   TCP
    *   UDP
    *   TCP/UDP

5. Enter the starting and ending port numbers. If the application uses a single port number, enter that number in both fields.

6. Click **Apply** to save your information and return to the previous screen.

Schedule for Firewall Rules

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

➢ **To specify the firewall rule schedule:**

1. Select **ADVANCED > Security > Schedule** to display the following screen:

2. Set up the schedule for blocking keywords and services.

    •   **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** 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 **All Day** for 24-hour blocking.

3. Select your time zone from the list. If you use daylight saving time, select the **Automatically adjust for daylight savings time** check box.

4. Click **Apply** to save your settings.

Security Event Email Notifications

To receive logs and alerts by email, provide your email information in the E-mail screen and specify which alerts you want to receive and how often.

➢ **To set up email notifications:**

1. Select **ADVANCED > Security > E-mail** to display the following screen:

2. To receive email logs and alerts from the WiFi modem router, select the **Turn E-mail Notification On** check box.

3. In the Your Outgoing Mail Server field, enter the name of your ISP outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration screen of your email program. When you leave this field blank, log and alert messages are not sent by email.

4. In the Send to This E-mail Address field, enter the email address to which logs and alerts are sent. This email address is also used for the From address. When you leave this field blank, log and alert messages are not sent by email.

5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.

6. You can have email alerts sent immediately when someone attempts to visit a blocked site and you can specify that logs are sent automatically.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, the log is cleared from the WiFi modem router's memory. If the WiFi modem router cannot email the log file, the log buffer might fill up. In this case, the WiFi modem router overwrites the log and discards its contents.

7. Click **Apply** to save your settings.

Administration

Manage your network

8

This chapter describes the settings for administering and maintaining your WiFi modem router and home network. See also:

- *Remote Management* on page 116 for information about upgrading or checking the status of your WiFi modem router over the Internet
- *Traffic Meter* on page 119 for information about monitoring the volume of Internet traffic passing through your WiFi modem router's Internet port

This chapter includes the following sections:

- *Upgrade the WiFi Modem Router Firmware*
- *View WiFi Modem Router Status*
- *View VPN Status*
- *View Logs of Web Access or Attempted Web Access*
- *Attached Devices*
- *Manage the Configuration File*
- *Set Password*
- *Diagnostics*

Upgrade the WiFi Modem Router Firmware

The WiFi modem router firmware (routing software) is stored in flash memory. You can update the firmware from the Administration menu on the Advanced tab. You might see a message at the top of the genie screens when new firmware is available for your product.

You can use the Check button on the Firmware Upgrade screen to check and update to the latest firmware for your product when new firmware is available.

➢ **To check for new firmware and update your WiFi modem router:**

1. Select **ADVANCED > Administration > Router Update** to display the following screen:
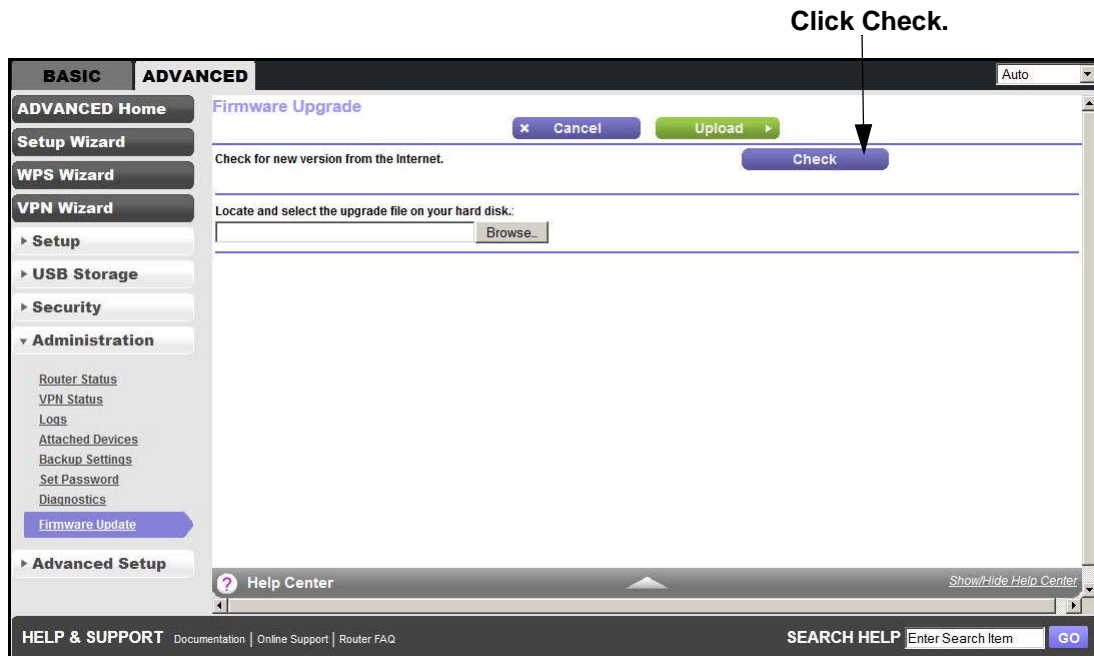
Click Check.

2. Click **Check**.

   The WiFi modem router finds new firmware information when any is available.

3. Click **Yes** to update and locate the firmware you downloaded (the file ends in .img).

⚠ **WARNING:**

When uploading firmware to the WiFi modem router, *do not* **interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.**

When the upload is complete, your WiFi modem router restarts. The upgrade process typically takes about one minute. Read the new firmware release notes to determine whether you need to reconfigure the WiFi modem router after upgrading.

View WiFi Modem Router Status

To view WiFi modem router status and usage information, select **ADVANCED Home**, or select **Administration > Router Status** to display the following screen:

Router Information

Hardware Version. The WiFi modem router model.

Firmware Version. The version of the WiFi modem router firmware. It changes if you upgrade the WiFi modem router firmware.

GUI Language Version. The localized language of the user interface.

LAN Port.

* **MAC Address**. The Media Access Control address. This address is the unique physical address used by the Ethernet (LAN) port of the WiFi modem router.

* **IP Address**. The IP address used by the Ethernet (LAN) port of the WiFi modem router. The default is 192.168.1.1.

* **DHCP Server**. Identifies whether the WiFi modem router's built-in DHCP server is active for the LAN-attached devices.

Internet Port

MAC Address. The Media Access Control address. This address is the unique physical address used by the Internet (WAN) port of the WiFi modem router.

IP Address. The IP address used by the Internet (WAN) port of the WiFi modem router. If no address is shown or the address is 0.0.0, the WiFi modem router cannot connect to the Internet.

Active Connection. This shows if the WiFi modem router is using a fixed IP address on the WAN. If the value is DHCP Client, the WiFi modem router obtains an IP address dynamically from the ISP.

IP Subnet Mask. The IP subnet mask used by the Internet (WAN) port of the WiFi modem router.

Domain Name Server. The Domain Name Server addresses used by the WiFi modem router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

Show Statistics Button

On the Router Status screen, in the Internet Port pane, click the **Show Statistics** button to display the following screen:

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	DHCP Client	203424	3697910	0	5299	164167	00:59:17
LAN1	Link down						
LAN2	Link down						
LAN3	Link down	--	--	--	--	--	--
LAN4	Link down						
WLAN b/g/n	145M	1123047	32128	0	93	1	839:04:59
WLAN a/n	450M	0	0	0	0	0	839:04:52

System Up Time 839:05:56

ADSL Link	Downstream	Upstream
Link Rate	0 Kbps	0 Kbps
Line Attenuation	0 dB	0 dB
Noise Margin	0 dB	0 dB

Poll Interval: 5 (secs)   Set Interval   Stop

Figure 10. System up time and poll interval statistics

System Up Time. The time elapsed since the WiFi modem router was last restarted.

Port. The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:

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

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

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

Connection Status Button

On the Router Status screen in the Internet Port pane, click the **Connection Status** button to view connection status information.

Figure 11. View connection status information

The Release button returns the status of all items to 0. The Renew button refreshes the items. The Close Window button closes the Connection Status screen.

IP Address. The IP address that is assigned to the WiFi modem router.

Subnet Mask. The subnet mask that is assigned to the WiFi modem router.

Default Gateway. The IP address for the default gateway that the WiFi modem router communicates with.

DHCP Server. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the WiFi modem router.

DNS Server. The IP address of the Domain Name Service server that provides translation of network names to IP addresses.

Lease Obtained. The date and time when the lease was obtained.

Lease Expires. The date and time that the lease expires.

Wireless Settings (2.4 GHz and 5 GHz)

The following settings are displayed:

Name (SSID). The wireless network name (SSID) used by the WiFi modem router. The default names for the 5 GHz ends in -5G to distinguish it from the 2.4-GHz network.

Region. The geographic region where the WiFi modem router is being used. It might be illegal to use the wireless features of the WiFi modem router in some parts of the world.

Channel. Identifies the operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the WiFi modem router finds the best operating

channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 do not interfere with each other.

Mode. Indicates the wireless communication mode: Up to 54 Mbps, Up to 130 Mbps (default), and Up to 300 Mbps.

Wireless AP. Indicates whether the radio feature of the WiFi modem router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates whether the WiFi modem router is broadcasting its SSID.

Wireless Isolation. Indicates whether wireless connections to the WiFi modem router are prevented.

Wi-Fi Protected Setup. Indicates whether Wi-Fi Protected Setup is configured for this network.

Guest Network (2.4 GHz and 5 GHz)

Name (SSID). The 11N wireless network name (SSID) used by the WiFi modem router. The default names are NETGEAR-Guest and NETGEAR-5G-Guest.

Wireless AP. Indicates whether the radio feature of the WiFi modem router is enabled. If this feature is not enabled, the Wireless LEDs on the front panel are off.

Broadcast Name. Indicates whether the WiFi modem router is broadcasting its SSID.

Wireless Isolation. Indicates whether wireless connections to the WiFi modem router are prevented.

Allow guest to access My Local Network. Indicates whether any user who connects to this SSID can access local networks associated with the WiFi modem router.

View VPN Status

The log is a detailed record of the websites you accessed or attempted to access. Up to 256 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

Select **ADVANCED > Administration > VPN Status**. The VPN Status/Log screen displays:
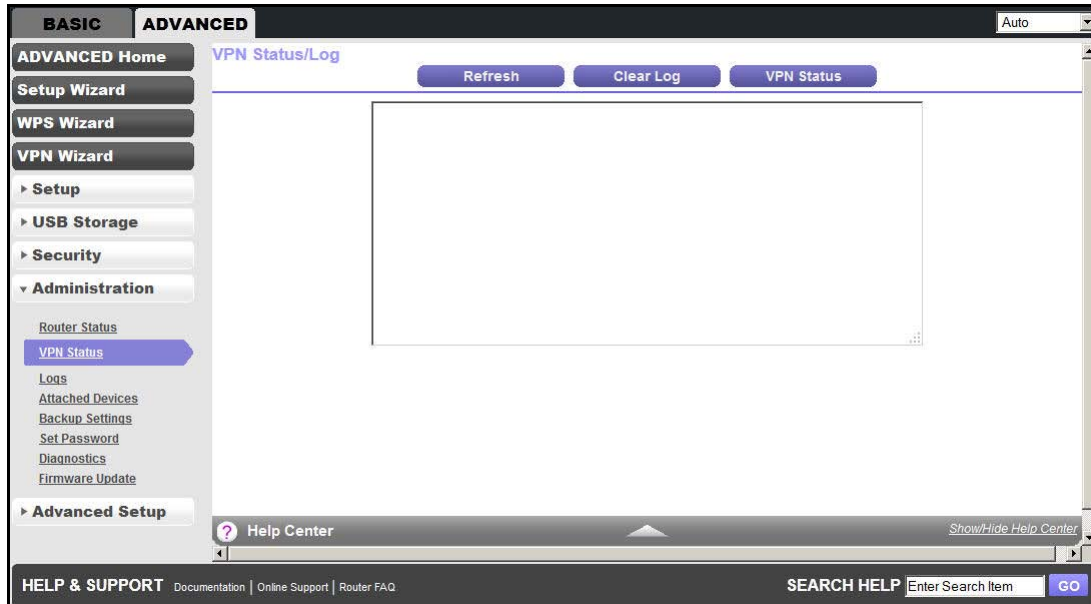
The VPN Status/Log screen shows the details of recent VPN activity.

To refresh the log screen, click the **Refresh** button.

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

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

View Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you accessed or attempted to access. Up to 256 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

Select **ADVANCED > Administration > Logs**. The Logs screen displays.
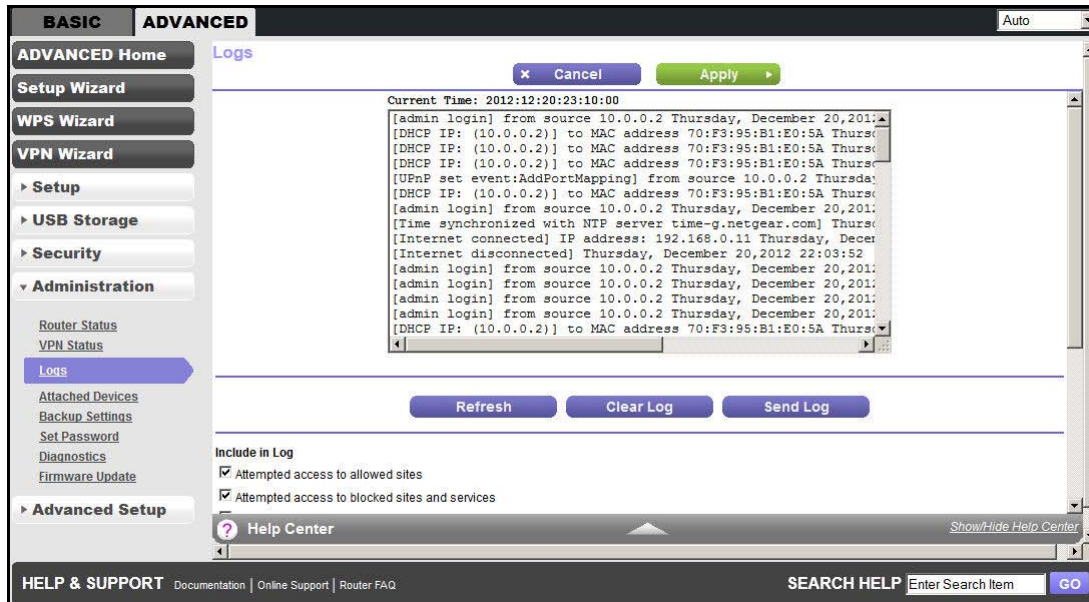
The Logs screen shows the following information:

- **Date and time**. The date and time the log entry was recorded.

- **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**. Whether the access was blocked or allowed.

- **Include in Log**. 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. When you have email notification on, you receive these logs in an email message. when you do not have email notification set up, you can view the logs here.

- **Syslog**. The logs can be sent to a syslog server. Enable one of these three options, as required:

  - **Disable**. Select this option when you do not have a syslog server.

  - **Broadcast on LAN**. The syslog data is broadcast rather than sent to a specific syslog server. Use this option when your syslog server does not have a fixed IP address.

  - **Send to this Syslog server IP address**. When your syslog server has a fixed IP address, select this option and enter the IP address of your syslog server.

To refresh the log screen, click the **Refresh** button.

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

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

To save your settings, click the **Apply** button.

Attached Devices

See *Attached Devices* on page 32.

Manage the Configuration File

The configuration settings of the WiFi Modem Router are stored within the WiFi modem 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 WiFi modem router's configuration settings:**

   1. Select **ADVANCED > Administration > Backup Settings** to display the following screen:
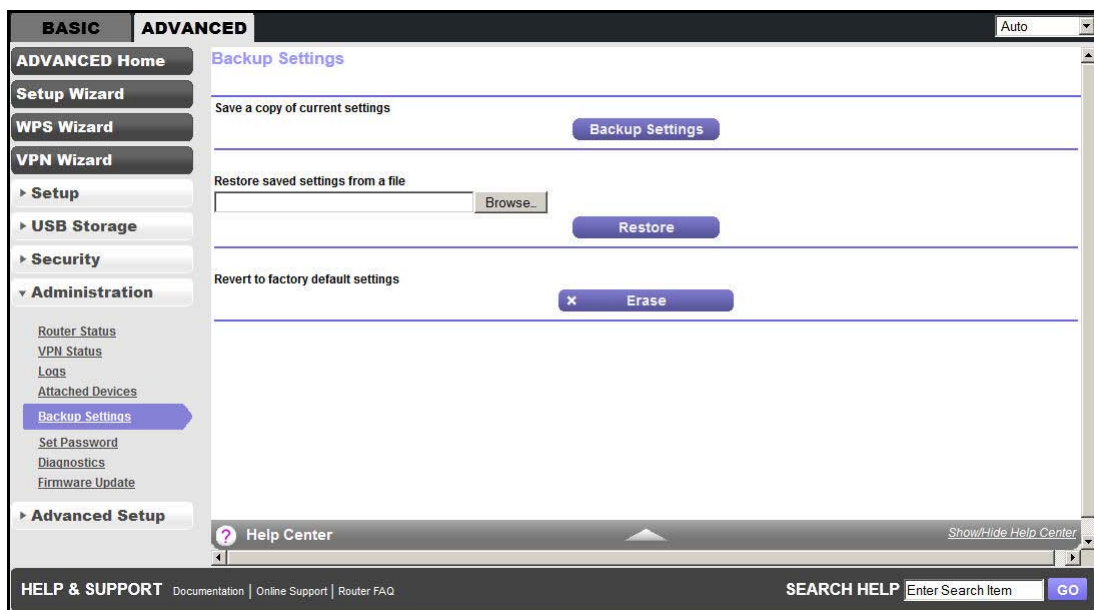
   2. Click **Backup Settings** to save a copy of the current settings.
   3. Choose a location to store the .cfg file that is on a computer on your network.

Restore Configuration Settings

➢ **To restore configuration settings that you backed up:**

   1. Enter the full path to the file on your network or click the **Browse** button to find the file.
   2. When you have located the .cfg file, click the **Restore** button to upload the file to the WiFi modem router.

Upon completion, the WiFi modem router reboots.

⚠️ **WARNING:**

Do not interrupt the reboot process.

Erase

Under some circumstances (for example, if you move the WiFi modem router to a different network or if you have forgotten the password), you might want to erase the configuration and restore the factory default settings.

Either you can use the Restore Factory Settings button on the back of the WiFi modem router (see *Factory Settings* on page 141), or you can click the **Erase** button in this screen.

Erase sets the user name to admin, the password to password, and the LAN IP address to 192.168.1.1, and enables the WiFi modem router's DHCP.

Set Password

This feature allows you to change the default password that is used to log in to the WiFi modem router with the user name **admin**.

This procedure is not the same as changing the password for wireless access. The label on the bottom of your WiFi modem router shows your unique wireless network name (SSID) and password for wireless access (see *Label* on page 12).

➢ **To set the password for the user name admin:**

1. Select **ADVANCED > Administration > Set Password** to display the following screen:

2. Type the old password and type the new password twice in the fields on this screen.

3. If you want to be able to recover the password, select the **Enable Password Recovery** check box.

4. Click **Apply** so that your changes take effect.

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 if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➢ **To set up password recovery:**

1. Select the **Enable Password Recovery** check box.

2. Select two security questions and provide answers to them.

3. Click **Apply** to save your changes.

When you use your browser to access the router, the login window displays. If password recovery is enabled, when you click Cancel, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

Diagnostics

You can perform various diagnostics. For normal operation, these tests are not required.

➢ **To perform diagnostic tests:**

1. Select **ADVANCED > Administration > Diagnostics** to display the following screen:
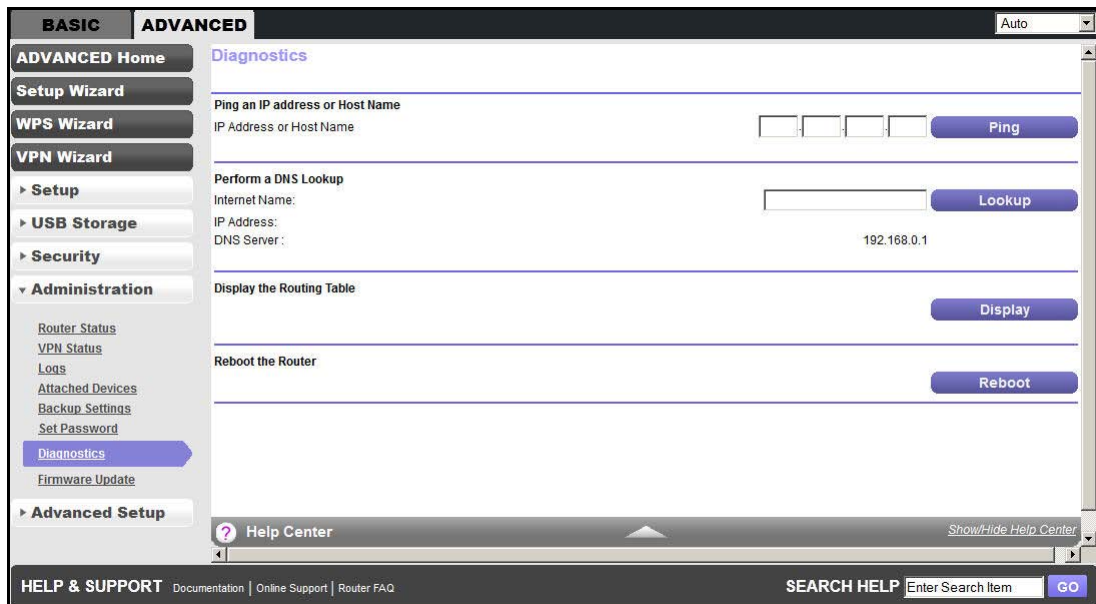
2. Perform the following diagnostics as needed:

- **Ping an IP address or Host Name**. Use this test to send a ping packet request to the specified IP address or host name. This test is often used to test a connection. If the request times out (in other words, no reply is received), this result usually means that the destination is unreachable. Note, however, that some network devices can be configured not to respond to a ping.

- **Perform a DNS Lookup**. A DNS (Domain Name Server) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a web, FTP, mail, or other server on the Internet, do a DNS lookup to find the IP address.

- **Display the Routing Table**. This operation displays the internal routing table.

- **Reboot the Router**. Click this button to perform a remote restart of the router. Use this operation if the router seems to have become unstable or is not operating normally.

> **Note:** Rebooting breaks any existing connections either to the router (such as this one) or through the router (LAN users accessing the Internet). However, connections to the Internet are automatically reestablished when possible.