NETGEAR®

R6200v2 Smart WiFi Router

User Manual

Support

Thank you for selecting NETGEAR products.

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

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

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

Trademarks

Contents

Chapter 8 Administration

Chapter 9 Advanced Settings

Chapter 10 Troubleshooting

Appendix A Supplemental Information

Appendix B Notification of Compliance

Hardware Setup

1

Getting to know your router

The R6200v2 Smart WiFi Router delivers next generation WiFi speeds with better range and speeds, up to 1200 Mbps.[1] It offers the best wireless coverage for large homes and is ideal for homes with eight or more wireless devices.

The router automatically uses NETGEAR Beamforming+ technology to enhance WiFi performance. Because it's automatic, you don't have to turn on Beamforming+ or configure it. When you connect to the WiFi network, Beamforming+ focuses on your location for even better WiFi performance and speed. Beamforming+ locks onto your laptop, tablet, or smartphone, and follows as you move from place to place, so you keep your optimal WiFi connection.

Compatible with next-generation WiFi devices and backward compatible with 802.11a/b/g/n devices, the router enables HD streaming throughout your home. With speeds of up to (300 Mbps + 867 Mbps) and simultaneous dual-band Wi-Fi technology, the router avoids wireless interference, ensuring top WiFi speeds and reliable connections. In addition, four Gigabit Ethernet ports offer ultra-fast wired connections. Wirelessly access and share a USB hard drive or USB printer using the USB 3.0 port.

If you already set up your router, you can skip this chapter. If you have not done that yet, this chapter covers the hardware setup. *Chapter 2, Getting Started*, explains how to access your router to view or change its settings.

This chapter contains the following sections:

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

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

---

1. Maximum wireless signal rate derived from IEEE standard 802.11 specifications. Actual data throughput and wireless coverage will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate and wireless coverage. NETGEAR makes no express or implied representations or warranties about this product's compatibility with any future standards.

Unpack Your Router

Open the box and remove the router, cables, and installation guide.

Ethernet cable with internal shielding

R6200v2 Smart WiFi Router   **Power adapter**
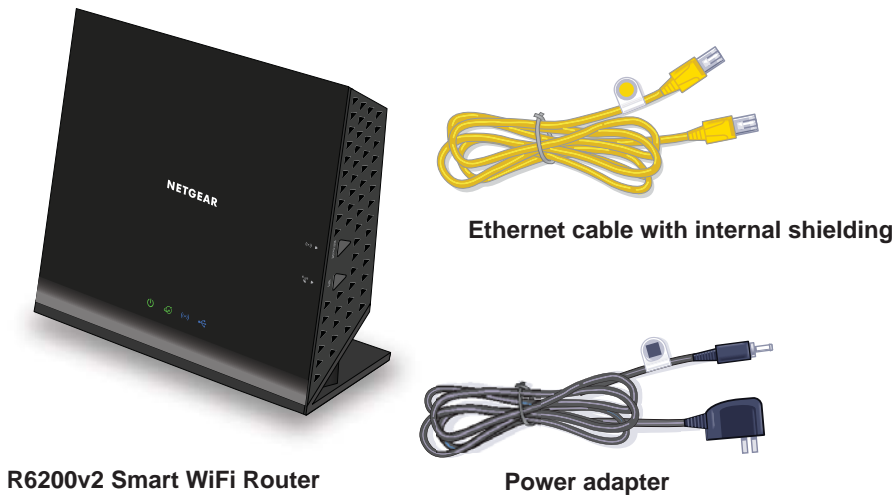
Figure 1. Check the package contents

Your box contains the following items:

- R6200v2 Smart WiFi Router
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable[2]
- Installation guide with cabling and router setup instructions

If any parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton and original packing materials, in case you return the product for repair.

Hardware Features

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

---

2. *All cables used to connect peripherals must be shielded and grounded. Operation with cables connected to peripherals that are not shielded and grounded may result interference to radio and television reception.*

Front and Side Panels

The router front and side panels have the status LEDs and buttons shown in the following figure.

WiFi On/Off button

WPS button

LEDs
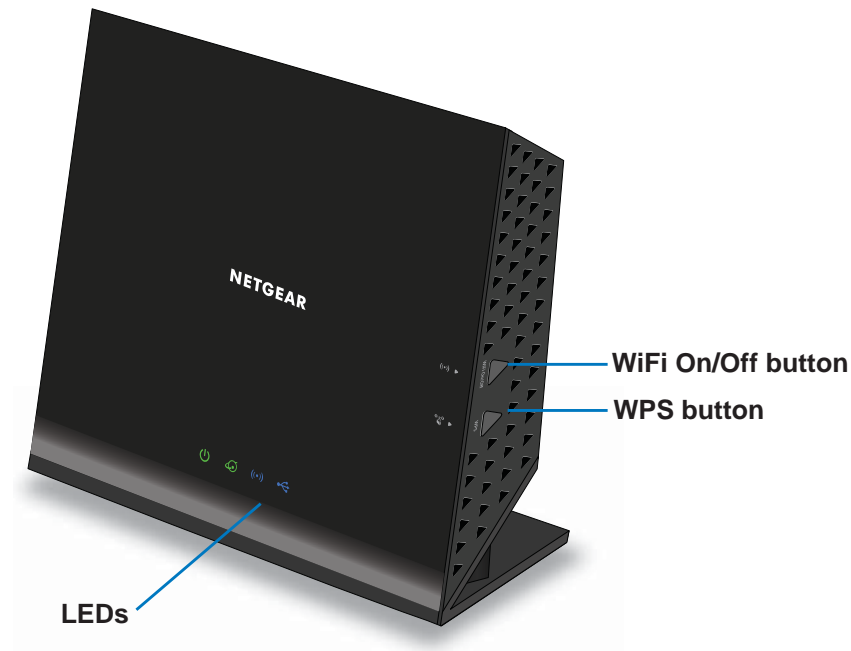
Figure 2. Router front and side view

Table 1. Front panel LED descriptions

LED	Description
Power	• **Solid amber**. The router is starting. • **Blinking amber**. The firmware is upgrading, or the Reset button was pressed. • **Solid green**. The router is ready. • **Blinking green**. The firmware is corrupted. Visit *www.netgear.com/support*. • **Off**. Power is not supplied to the router.
Internet	• **Solid green**. The Internet connection is ready. • **Solid amber**. The Ethernet cable connection to the modem has been detected. • **Off**. No Ethernet cable is connected to the modem.
Wireless	• **Solid blue**. The wireless radio is operating in either 2.4 GHz or 5 GHz mode. • **Blinking**. The router is in WPS mode. • **Off**. The wireless radios are off for both 2.4 GHz and 5 GHz.
USB	• **Solid blue**. The router has accepted the USB device. The USB device is ready to be used. • **Blinking blue**. A USB device is plugged in and is trying to connect. • **Off**. No USB device is connected;, or someone clicked the Safely Remove Hardware button, and it is now safe to remove the attached USB device.

The WiFi and WPS buttons toggle the WiFi and WPS functions on and off.

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

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

Rear Panel

The rear panel has the connections and buttons shown in the following figure.
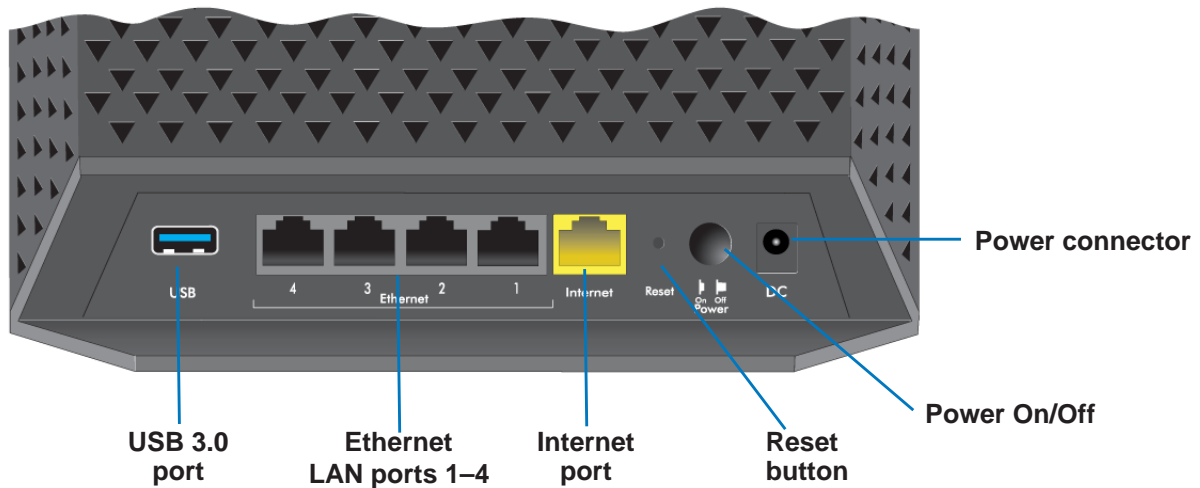
Figure 3. Router rear panel

The Reset button restores the factory settings. See *Factory Settings* on page 126.

Label

The label on the router shows the login information, MAC address, and serial number.

Default access information

Preset WiFi password

Serial number and MAC address
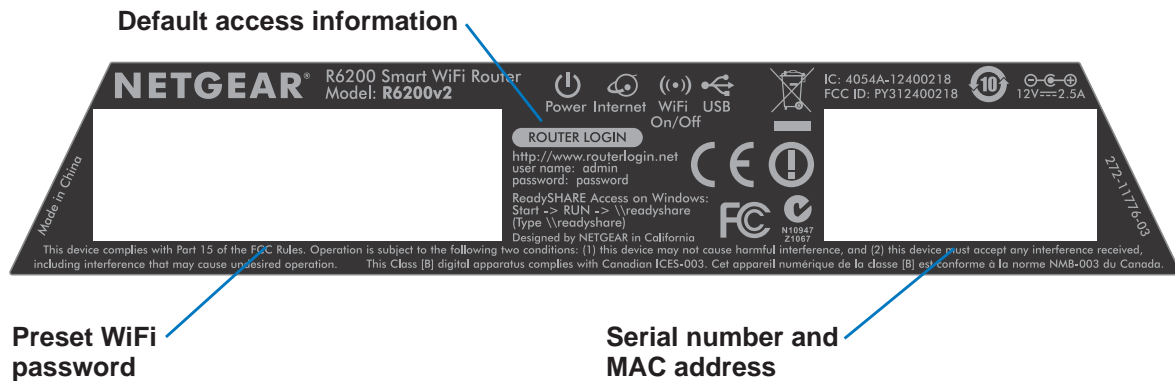
Figure 4. The label shows unique information about your router

Position Your Router

The 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 router and your other devices to a minimum.

- Away from electrical devices that are potential sources of interference. Equipment that might cause interference includes ceiling fans, home security systems, microwaves, computers, the base of a cordless phone, or a 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.

Getting Started

Connecting to the router

<div align="right">2</div>

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

This chapter contains the following sections:

- *Router Setup Preparation*
- *Login and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie After Installation*
- *Upgrade the Firmware*
- *Dashboard (BASIC Home Screen)*
- *Join Your Wireless Network*
- *NETGEAR genie App and Mobile genie App*

Router Setup Preparation

You can set up your router with the NETGEAR genie automatically, or you can use the genie menus and screens to set up your router manually. Before you start the setup process, get your ISP information and make sure the computers and 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, 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 router and to check that your Internet configuration is correct. When your Internet service starts, your Internet service provider (ISP) typically gives you all 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 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 setting 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 that the router uses.

Login and Access

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

- **Router login**. The user name admin logs you in to the router interface. For details about this login, see *Use NETGEAR genie After Installation* on page 15.
- **ISP login**. The login that your ISP provided logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network key or password**. Your router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label on the bottom of your router.

NETGEAR genie Setup

NETGEAR genie runs on any device with a web browser. Installation with basic setup takes about 15 minutes to complete.

➢ **To use NETGEAR genie to set up your router:**

1. Turn the router on by pressing the **On/Off** button.

2. Make sure that your computer or wireless device is connected to the router with an Ethernet cable (wired) or wirelessly with the preset security settings listed on the bottom label.

3. Launch your Internet browser.

   - The first time you set up the Internet connection for your router, the browser goes to http://www.routerlogin.net, and the NETGEAR genie screen displays.

   NETGEAR genie™
   R6200v2

   Configuring the Internet Connection

   You are not yet connected to the Internet.

   Do you want NETGEAR Genie to help?
   - Yes
   - No, I want to configure the Internet connection myself.
   - I have saved the router settings in a file and I want to restore the router to those settings.

   Next
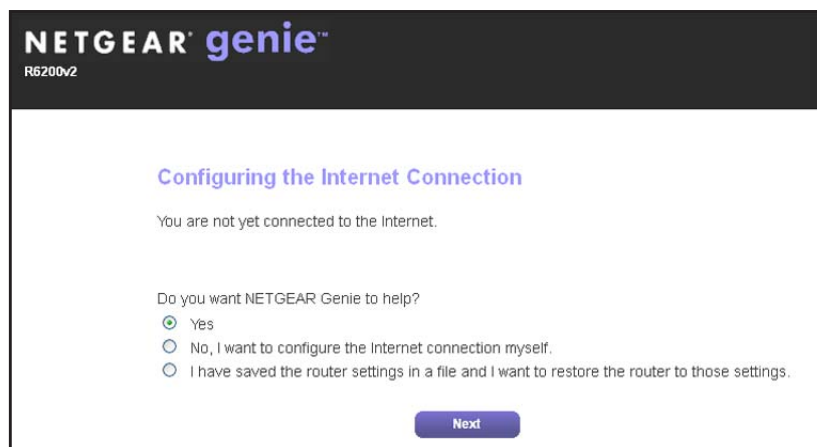
   - If you already used the NETGEAR genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR genie screen. See *Use NETGEAR genie After Installation* on page 15.

4. Follow the onscreen instructions.

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

If the browser cannot display the web page:

- Make sure that the computer is connected to one of the four LAN Ethernet ports or wirelessly to the router.

- Make sure that the router has full power, and that its WiFi LED is lit.

- Close and reopen the browser or clear the browser cache.

- Browse to **http://www.routerlogin.net**.

- If the computer is set to a static or fixed IP address (this setting is uncommon), change it to obtain an IP address automatically from the router.

If the router does not connect to the Internet:

1. Review your settings. Make sure that you have selected the correct options and typed everything correctly.

2. Contact your ISP and 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 router, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the router. If you want to view or change settings for the router, you can use genie again.

➢ **To log in to the router:**

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

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

   A login window displays.

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

The router user name and password are different from the user name and password for logging in to your Internet connection. For more information, see *Login and Access* on page 13.

Upgrade the Firmware

When you set up your router and connect to the Internet, the router automatically checks to see if newer firmware is available. If it is, a message is displayed on the top of the screen.

➢ **To upgrade the firmware:**

1. Click the message that tells you new firmware is available.

   During the firmware upgrade, you cannot access the Internet.

2. Click the **Yes** button to upgrade the router with the latest firmware.

⚠ **WARNING:**

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

After the upgrade, the router restarts.

For more information, see *Update the Router Firmware* on page 81.

Dashboard (BASIC Home Screen)

The 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 and change the settings. The left column has menus. You can use the ADVANCED tab to access more menus and screens.
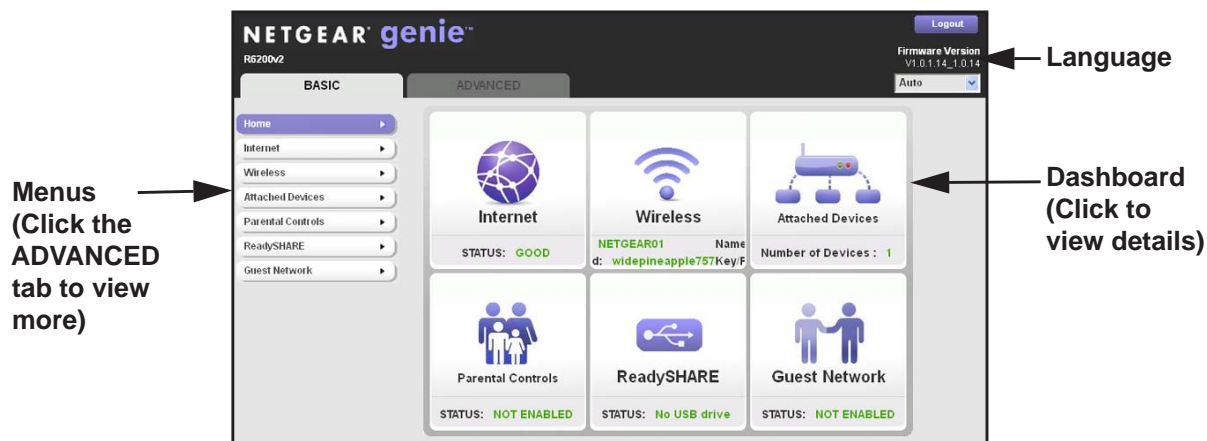
Figure 5. Basic Home screeN

- **Home**. This dashboard screen displays when you log in to the router.
- **Internet**. Set, update, and check the ISP settings of your router.
- **Wireless**. View or change the wireless settings for your 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 router, then it is displayed here.
- **Guest Network**. Set up a guest network to allow visitors to use your router's Internet connection.
- **ADVANCED tab**. Set the 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*. You need a solid understanding of networking to use this tab.
- **Help & Support**. Visit the NETGEAR support site for information, help, and product documentation. These links work once you have an Internet connection.

Join Your Wireless Network

You can use the manual or the WPS method to join your wireless network. For instructions about how to set up a guest network, see *Set Up a Guest Network* on page 28.

Manual Method

With the manual method, choose the network that you want and type its password to connect.

➢ **To connect manually:**

1. On your computer or wireless device, open the software that manages your wireless connections.

   This software scans for all wireless networks in your area.

2. Look for your network and select it.

   The unique WiFi network name (SSID) and password are on the router label. If you changed these settings, look for the network name that you used.

3. Enter the router password and click the **Connect** button.

Wi-Fi Protected Setup Method

Wi-Fi Protected Setup (WPS) lets you connect to a secure WiFi network without typing its password. Instead, press a button or enter a PIN. NETGEAR calls WPS Push 'N' Connect.

Some older WiFi equipment is not compatible with WPS. WPS works only with WPA2 or WPA wireless security.

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

1. Press the **WPS** button on the side of the router.

2. Within two minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device.

   The WPS process automatically sets up your wireless computer with the network password and connects you to the wireless network.

NETGEAR genie App and Mobile genie App

The genie app is the easy dashboard for managing, monitoring, and repairing your home network. For information about the genie apps, see the *NETGEAR genie App User Manual* .

Retrieve wireless password

About genie

Menu

Language

Dashboard (Click to view details)

Support

Figure 6. genie app dashboard

The genie app can help you with the following:

- Automatically repair common wireless network problems.
- Have easy access to router features like Live Parental Controls, guest access, Internet traffic meter, speed test, and more.

The genie mobile app works on your iPhone, iPad, or Android phone:

Phone status

Log in to the router

Search NETGEAR support

Information about genie mobile app and the connected router
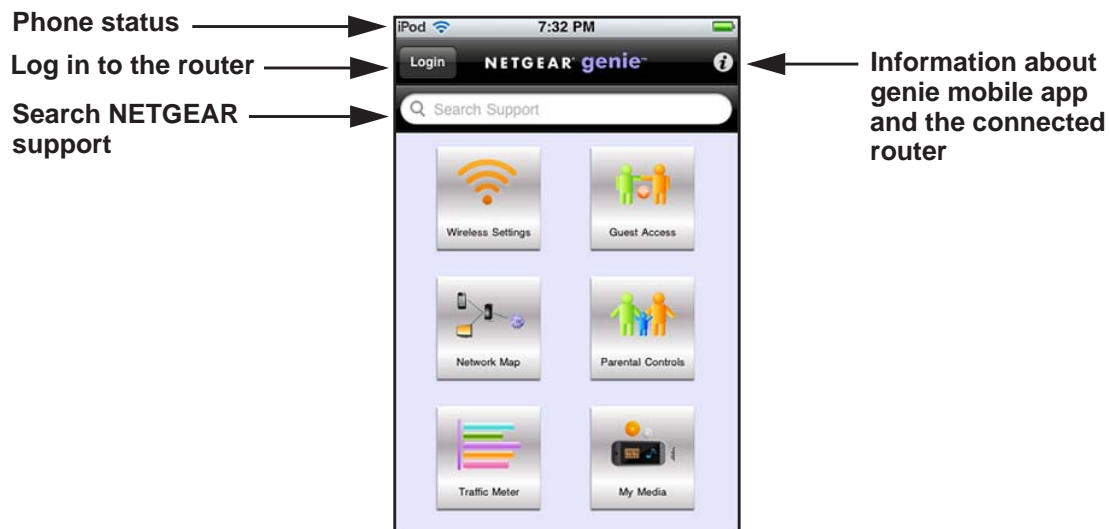
Figure 7. genie mobile app home screen

Basic Settings 3

Your Internet connection and WiFi network

This chapter describes the steps in setting up the router using genie. This chapter contains the following sections:

- *Internet Setup*
- *Parental Controls*
- *Basic Wireless Settings*
- *Set Up a Guest Network*
- *View Attached Devices*

For information about the ReadySHARE feature on the BASIC Home tab, see *Chapter 5, USB Storage* and *Chapter 6, ReadySHARE Printer*.

Internet Setup

The Internet Setup screen is where you view or change basic ISP information.

Note: You can use the Setup Wizard to detect the Internet connection and automatically set up the router. See *Internet Connection Setup Wizard* on page 31.

➢ **To view or change the basic Internet setup:**

1. Log in to the router (see *Use NETGEAR genie After Installation* on page 15).

    The BASIC Home screen displays.

2. Select **Internet**.

Scroll to view more settings
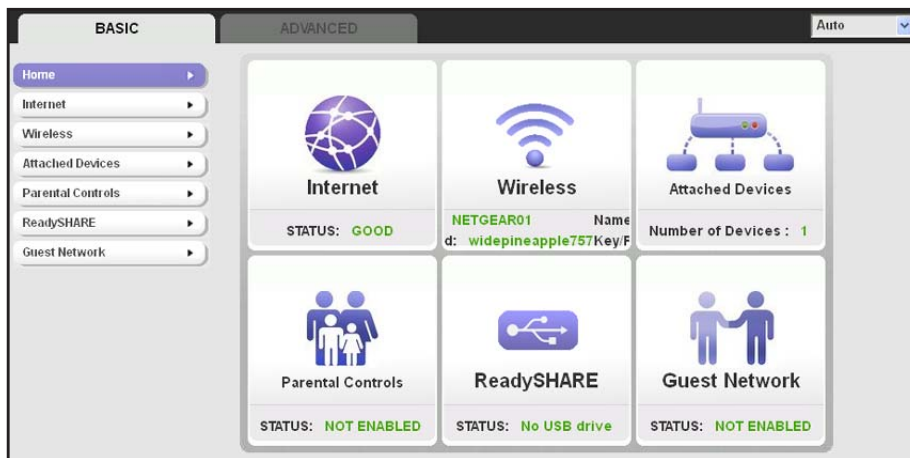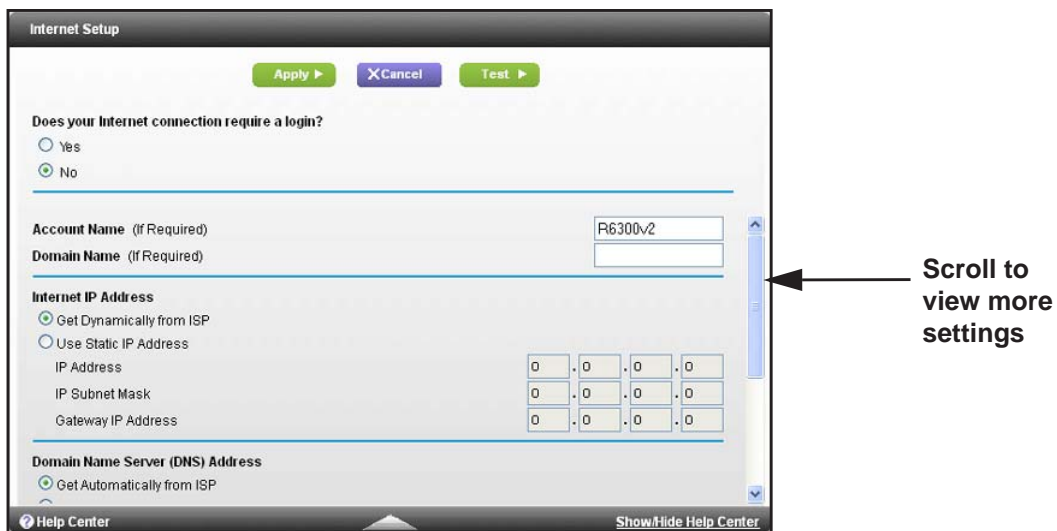
The fields that display in the Internet Setup screen depend on whether your Internet connection requires a login.

3. Select the **Yes** or **No** radio button.
    - **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.

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

    The default settings usually work fine. If you have problems with your connection, check the ISP settings.

5. Click the **Apply** button.

    Your settings are saved.

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

    If the NETGEAR website does not display within one minute, see *Chapter 10, Troubleshooting*.

The following descriptions explain all of the possible fields in the Internet Setup screen. The fields that display in this screen depend on whether tan ISP login is required.

Does Your Internet connection require a login? Select either the **Yes** or **No** radio button.

These fields display when no login is required:

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

These fields display when your ISP requires a login:

- **Internet Service Provider**. PPPoE or PPPoA.
- **Login**. The login name provided by your ISP. This login name is often an email address.
- **Password**. The password that you use to log in to your ISP.
- **Service Name (if Required)**. If your ISP provided a service name, enter it here.
- **Connection Mode**. Always On, Dial on Demand, or Manually Connect.
- **Idle Timeout (In minutes)**. If you want to change the login time-out, enter a new value in minutes. This setting determines how long the router keeps the Internet connection active when there is no Internet activity from the LAN. A value of 0 (zero) means never log out.

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 router to which your router connects.

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

- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.

- **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

NAT (Network Address Translation). NAT allows computers on your home network to share the router Internet connection. NAT is enabled by default because it is needed in most situations. The following settings are available:

- Enable
- Disable

Router MAC Address. The Ethernet MAC address that the router uses on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your router to use your computer's MAC address (also called cloning).

- **Use Default Address**. Use the default MAC address.

- **Use Computer MAC Address**. The router captures and uses the MAC address of the computer that you are now using. You have to use the one computer that the ISP allows.

- **Use This MAC Address**. Enter the MAC address that you want to use.

Parental Controls

The first time you select Parental Controls from the Basic Home screen, your browser goes to the Live Parental Controls website. You can learn more about Live Parental Controls or download the application.

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

1. Select **Parental Controls** on the dashboard screen.

2. Click either the **Windows Users** or **Mac Users** button.

3. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management utility.

   After installation, Live Parental Controls automatically starts.
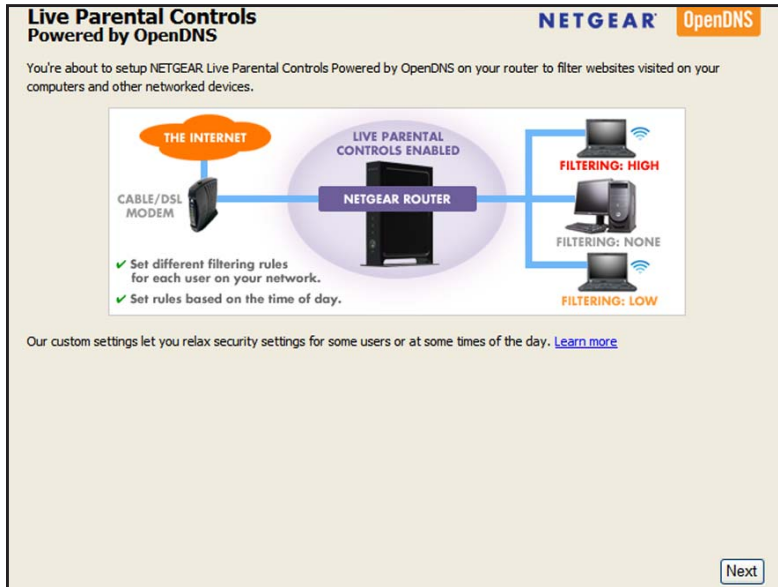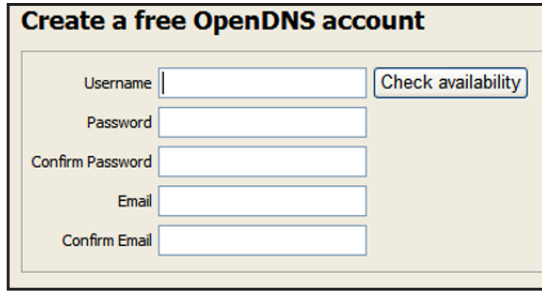
4. Click the **Next** button, read the note, and click the **Next** button again to proceed.

   Because Live Parental Controls uses free OpenDNS accounts, you are prompted to log in or create a free account.
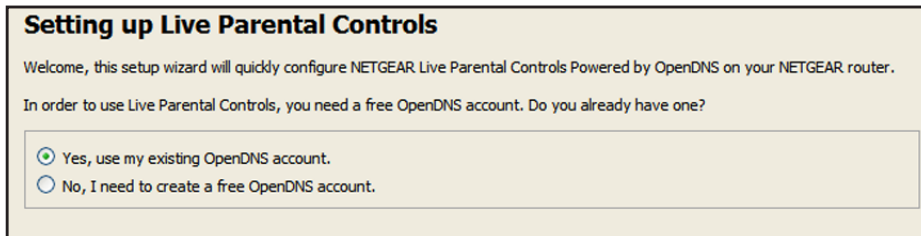
5. Select the radio button that applies to you and click the **Next** button.
   - If you already have an OpenDNS account, leave the **Yes** radio button selected.
   - If you do not have an OpenDNS account, select the **No** radio button.

If you are creating an account, the following screen displays:
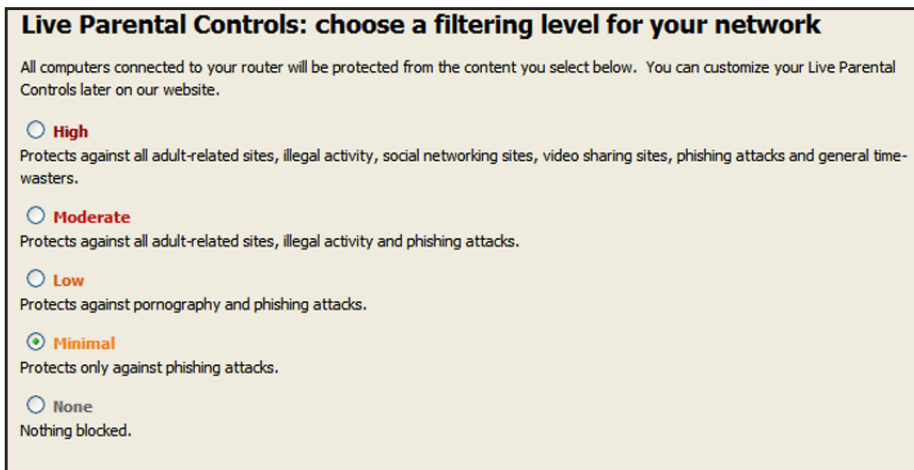
- Fill in the fields and click the **Check availability** button.

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

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

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

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

Basic Wireless Settings

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

The router comes with preset security. This means that the Wi-Fi 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 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 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 the Apply button. To avoid this problem, use a computer with a wired connection to access the router.

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

1. Select **BASIC > Wireless**.

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

2. Change the settings as needed.

3. Click the **Apply** button.

   Your settings are saved.

   If you were connected wirelessly to the router and you changed the SSID or wireless security, you are disconnected from the network.

4. If you changed the settings, make sure that you can connect wirelessly to the network with its new settings.

   If you cannot connect wirelessly, check the following:

   • Is your computer or wireless device connected to another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.

   • Is your computer or wireless device trying to connect to your network with its old settings (before you changed the settings)? If so, update the wireless network selection in your computer or wireless device to match the current settings for your network.

Wireless Settings Screen Fields

You can use this screen to view or change the wireless network settings and the security option.

• **Enable SSID Broadcast**. This feature allows the router to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default. To turn off the SSID broadcast, clear this check box, and click the **Apply** button.

• **Enable Wireless Isolation**. If this check box is selected, computers or wireless devices that join the network can use the Internet, but cannot access each other or access Ethernet devices on the network.

• **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.*

• **Region**. The location where the 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.

• **Channel**. The wireless channel the router uses. For 2.4 GHz, select a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

   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 four channels (for example, use Channels 1 and 5, or 6 and 10).

• **Mode**. For 2.4 GHz, Up to 145 Mbps is the default setting, which allows 802.11n and 802.11g wireless devices to join the network. The other settings are Up to 54 Mbps, and Up to 300 Mbps.

   At 5 GHz, Up to 867 Mbps is the default setting, which allows 802.11ac and 802.11a wireless devices to join the network. The other settings are Up to 173 Mbps and Up to 400 Mbps.

- **Security Options**. The router comes with unique preset wireless security. These settings are on the product label. NETGEAR recommends that you use preset security so that you can refer to the label if you forget the WiFi password. However, you can change the security option and passphrase.

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. Wi-Fi Protected Access (WPA) has several options including pre-shared key (PSK) encryption.

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

WPA uses a passphrase for authentication and to 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 works with all wireless network interface cards, but not all wireless access points.

WPA2-PSK is stronger than WPA-PSK. It is advertised to be theoretically 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. For help with WPA settings on your wireless computer or device, see the instructions that came with your product.

Change the Wireless Security Option

Your router is preset with unique wireless security settings. You can change the settings if you want. *NETGEAR recommends that you do not disable security.*

➢ **To change the WPA settings:**

1. Select **BASIC > Wireless Settings**.
2. Under Security Options, select the WPA option you want.

   Security Options
   ○ None
   ○ WPA-PSK [TKIP]
   ◉ WPA2-PSK [AES]
   ○ WPA-PSK [TKIP] + WPA2-PSK [AES]
   ○ WPA/WPA2 Enterprise
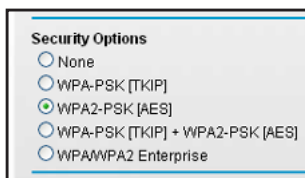
3. In the Passphrase field that displays when you select a WPA security option, enter the network key (password) that you want to use. It is a text string from 8 to 63 characters.
4. Write down the new password and keep it in a secure place for future reference.
5. Click the **Apply** button.

   Your changes are saved.

Set Up a Guest Network

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. Select **BASIC > Guest Network**.
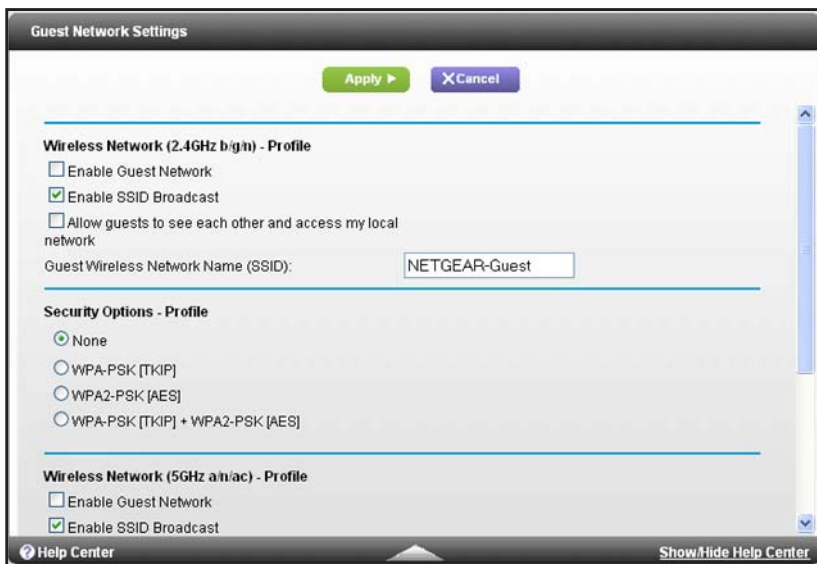
2. Select any of the following wireless settings:

   - **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, anyone who connects to this SSID has access to your local network, not just Internet access.

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 SSID.

4. Select a security option from the list.

   The security options are described in *Wireless Settings Screen Fields* on page 26.

5. Click the **Apply** button.

   Your settings are saved.

View Attached Devices

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

➢ **To go to the Attached Devices screen:**

1. From the Basic Home screen, select **Attached Devices**.

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

- **#** (number). The order in which the device joined the network.
- **IP Address**. The IP address that the router assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.
- **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.

2. Click the **Refresh** button to update this screen.

ADVANCED Home Settings

4

Specifying custom settings

This chapter helps you configure the advanced settings in your router using genie. This chapter contains the following sections:

- *NETGEAR genie Advanced Home Screen*
- *Internet Connection Setup Wizard*
- *WAN Setup*
- *LAN Setup*
- *WPS Wizard for WiFi Connections*
- *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*.

NETGEAR genie Advanced Home Screen

The genie Advanced Home screen presents status information. The content is the same as what is on the Router Status screen available from the Administration menu. See *View Router Status* on page 82.

Internet Connection Setup Wizard

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

➢ **To use the Setup Wizard:**

1. Select **ADVANCED > Setup Wizard**.

2. Select the **Yes** button.

   If you select No, you are taken to the Internet Setup screen (see *Internet Setup* on page 20).

3. Click the **Next** button.

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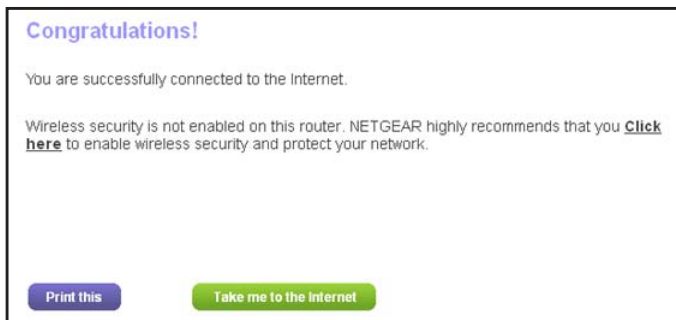
WAN Setup

The WAN Setup screen lets you configure advanced settings for the Internet port.

➢ **To view or change the WAN settings:**

1. Select **ADVANCED > Setup > WAN Setup**.

2. Specify the following settings:
   - **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, 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*.
   - **Respond to Ping on Internet Port**. If you want the router to respond to a ping from the Internet, select this check box. Use this setting only as a diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.

- **Disable IGMP Proxying**. IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. If you do not need this feature, you can select this check box to disable it.

- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. Reduce the MTU only if you are sure that it is necessary for your ISP connection. See *Change the MTU Size* on page 34.

- **NAT Filtering**. Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a 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 working. Open NAT provides a less secure firewall, but allows almost all Internet applications to work.

3. Click the **Apply** button.

   Your changes are saved.

Default DMZ Server

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

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

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

➢ **To set up a default DMZ server:**

1. Select **ADVANCED > Setup > WAN Setup**.
2. Select the **Default DMZ Server** check box.
3. Type the IP address.
4. Click the **Apply** button.

   Your change takes effect.

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 a 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. In some situations, changing the value fixes one problem but causes 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. For example, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

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

Table 2. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.

Table 2. Common MTU sizes (continued)

MTU	Application
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 value from 64 to 1500.

3. Click the **Apply** button.

   Your change is saved.

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

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

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

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

➢ **To change the LAN settings:**

1. Select **ADVANCED > Setup > LAN Setup**.

2. Enter the settings that you want to customize.

    These settings are described in the following sections.

3. Click the **Apply** button.

    Your changes are saved.

LAN TCP/IP Setup

- **IP Address**. The LAN IP address of the router.
- **IP Subnet Mask**. The LAN subnet mask of the 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 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 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 DHCP Server

For most home networks, this check box is selected so that the router acts 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 router.
- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the 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 router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings. See *Set Up Address Reservation* on page 38.

Role of the Router as a DHCP Server

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

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

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

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

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

➢ **To disable the DHCP server feature in the router:**

1. Select **ADVANCED > Setup > LAN Setup**.
2. Clear the **Use Router as DHCP Server** check box.
3. Click the **Apply** button.

4. (Optional) If this service is disabled and no other DHCP server is on your network, set your computer IP addresses manually so that they can access the router.

Set Up Address Reservation

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

➢ **To reserve an IP address:**

1. Select **ADVANCED > Setup > LAN Setup**.

2. In the Address Reservation section of the screen, click the **Add** button.

3. In the IP Address field, type the IP address to assign to the computer or server.

   Choose an IP address from the router's LAN subnet, such as 192.168.1.x.

4. 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.

5. Click the **Apply** button.

   The reserved address is entered into the table.

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

➢ **To edit or delete a reserved address entry:**

1. Select the radio button next to the reserved address you want to edit or delete.

2. Click the **Edit** button and make changes, or click the **Delete** button.

WPS Wizard for WiFi Connections

The WPS Wizard helps you add a wireless computer or device to your WiFi network without typing the WiFi password.

➢ **To use the WPS Wizard:**

1. Select **ADVANCED > WPS Wizard**.

2. Click the **Next** button.
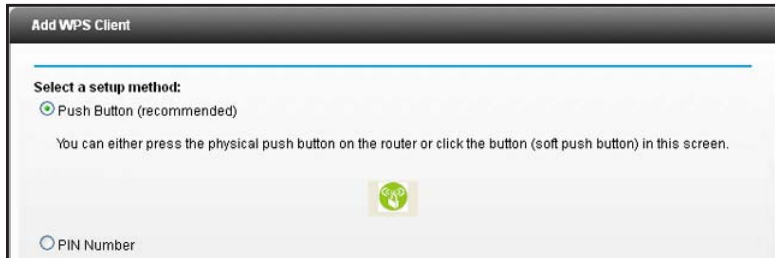
3. Select the radio button for the setup method that you want to use.
   - **Push button**. Either click the **WPS** button on this screen, or press the **WPS** button on the side of the router. Within two minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.
   - **PIN Number**. The screen adjusts.

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

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

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 router can provide QoS prioritization over the wireless link and on the Internet connection.

WMM QoS for Wireless Multimedia Applications

The 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 it and the client running that application have to have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video. WMM QoS is enabled by default.

➢ **To disable WMM QoS:**

1. Select **ADVANCED > Setup > QoS Setup**.

2. Clear the **Enable WMM** check box for the band (2.4 GHz or 5 GHz).

3. Click the **Apply** button.

Set Up Bandwidth Control

➢ **To set up the maximum uplink bandwidth:**

1. Select **ADVANCED > Setup > QoS Setup**.

2. Leave the **Enable WMM** check boxes selected.

3. (Optional) To prioritize Internet traffic, select the **Turn Internet Access QoS On** check box.

4. (Optional) To detect the current uplink bandwidth, click the **Check** button.

   This helps you to determinate the maximum bandwidth setting

5. Select the **Turn Bandwidth Control On** check box.

6. Use one of these methods to specify the maximum bandwidth:
   • To use the current uplink bandwidth, select the **Uplink bandwidth** radio button.
   • Select the **Automatically check Internet uplink bandwidth** radio button.

7. Click the **Apply** button.

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 router
- A specific device by MAC address

To specify prioritization of traffic, create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Priority Rules 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. Select **ADVANCED > Setup > QoS Setup**.
2. Select the **Turn Internet Access QoS On** check box.
3. Click the **Set Up QoS rule** button.

   The QoS Priority Rule list displays.

4. To add a priority rule, scroll down and click the **Add Priority Rule** button.

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

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

   A list of applications or games displays.

7. Scroll and select **Add a New Application**, or **Add a New Game**, as applicable.

8. If prompted, in the Connection Type list, select either **TCP, UDP,** or **TCP/UDP** (both). Specify the port number or range of port numbers that the application or game uses.

9. From the Priority list, select the priority for Internet access for this traffic relative to other applications and traffic.

   The options are Low, Normal, High, and Highest.

10. Click the **Apply** button.

   The rule is saved in the QoS Policy list.

QoS for a Router LAN Port

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

1. Select **ADVANCED > Setup > QoS Setup**.

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

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

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

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

6. From the QoS Policy for list, select the LAN port.

---

7. From the Priority list, select the priority for Internet access for this port's traffic relative to other applications.

   The options are Low, Normal, High, and Highest.

8. Click the **Apply** button.

   The rule is saved in the QoS Policy list.

9. Click the **Apply** button.

QoS for a MAC Address

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

1. Select **ADVANCED > Setup > QoS Setup**.

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

   The QoS - Priority Rules screen displays.

3. Click **Add Priority Rule**.

4. From the Priority Category list, select **MAC Address**.

5. If the device to be prioritized appears in the MAC Device List, select its radio button.

   The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click the **Refresh** button. If it still does not appear, fill in these fields manually.

6. From the Priority list, select the priority for Internet access for this device's traffic relative to other applications and traffic.

   The options are Low, Normal, High, and Highest.

7. Click the **Apply** button.

   This rule is saved in the QoS Policy list.

   The QoS Setup screen displays.

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

9. Click the **Apply** button.

Edit or Delete a QoS Policy

➢ **To edit or delete a QoS policy:**

1. Select **ADVANCED > QoS Setup**.

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

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

    •   Click the **Edit** button to edit the QoS policy and change the policy settings.

3. Click the **Apply** button.

    Your changes are saved.

USB Storage 5

Accessing and configuring a USB storage Device

This chapter describes how to access and configure a USB storage drive attached to your router. The USB port on the router can be used to connect only USB storage devices like flash drives or hard drives, or a printer. Do not connect computers, USB modems, CD drives, or DVD drives to the router USB port.

This chapter contains the following sections:

- *Connect a USB Storage Device to the Router*
- *Safely Remove a USB Drive*
- *Access the USB Storage Device*
- *Sharing Files*
- *View a USB Device Attached to the Router*
- *USB Storage Device Network and Access Settings*
- *Available Network Folders*
- *Specify Approved USB Devices*
- *Media Server Settings*
- *TiVo Support*

For information about using the ReadySHARE Printer feature, see *Chapter 6, ReadySHARE Printer*.

For more information about ReadySHARE features, visit *www.netgear.com/readyshare*.

Connect a USB Storage Device to the Router

ReadySHARE lets you access and share or a USB drive connected the router USB port. If your USB device has special drivers, it is not compatible.

➢ **To connect a USB storage device:**

1. Insert your USB storage device into the USB port on the rear panel of the router.
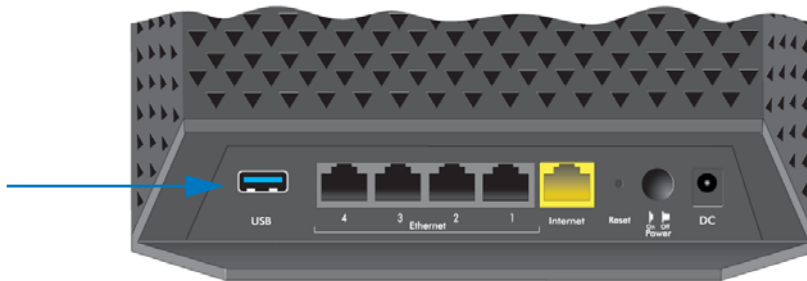
2. If your USB device has a power supply, you must use it when you connect the USB device to the router.

   It might take up to 2 minutes before the USB device is ready for sharing.

Safely Remove a USB Drive

If you want to physically disconnect a USB drive from the router USB port, first, log in to the router, and then safely remove the USB device.

➢ **To remove a USB drive safely:**

1. Select **USB Storage > Basic Settings**.

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

   This takes the drive offline.

3. Physically disconnect the USB drive.

Access the USB Storage Device

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

➢ **To access the USB device from a Mac:**

1. Select **Go > Connect to Server**.

2. Enter **smb://readyshare** as the server address.

3. Click the **Connect** button.

➢ **To access the USB device from a Windows computer:**

Use any of these methods:

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

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

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

   The readyshareconnect.exe file is downloaded to your computer.

3. Launch readyshareconnect.exe.
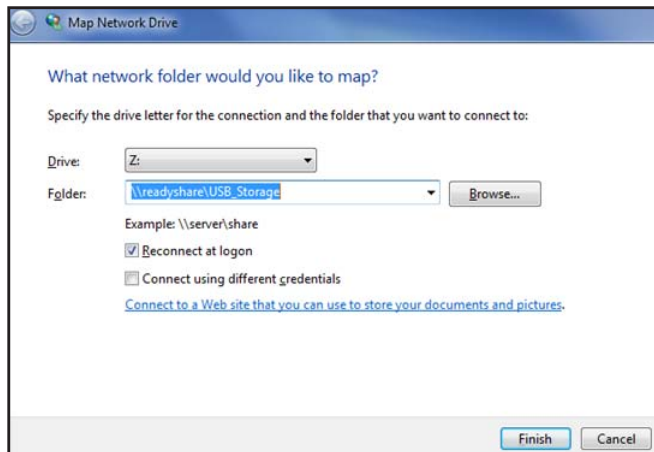
4. Select the drive letter that you want to map to the network folder.
5. (Optional) If you want to connect to the USB drive as a different user, select the **Connect using different credentials** check box.

   a. Type the user name and password that you want to use.

   b. Click the **OK** button.

6. Click the **Finish** button.

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

➢ **To access the USB drive from a remote computer:**

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

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

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

1. Make sure that the FTP check box is selected in the Access Method section of the USB Storage (Advanced Settings) screen (see *USB Storage Device Network and Access Settings* on page 51).

2. Launch a web browser.

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

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

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

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

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

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

Sharing Files

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be Windows, Mac, or Linux file types NTFS, Ext 3, FAT 32,including text, Word, PowerPoint, Excel, MP3, pictures, and multimedia files. USB drive applications include:

• Sharing multimedia with friends and family such as MP3 files, pictures, and other multimedia with local and remote users.

• Sharing resources on your network. You can store files in a central location so that you do not have 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 method 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 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 Device Network and Access Settings* on page 51.

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 Windows computer, but not shared on the network.
*   The Mac and the Windows computer are not visible to each other on the network.

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

*   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.
*   On the Window computer, use a web browser or Microsoft Networking to copy the files from the USB drive to the 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 router allows you to share large files such as PowerPoint presentations or .zip files over the Internet. FTP can be used to download shared files from the router.

Sharing files with a remote colleague involves the following considerations:

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

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

View a USB Device Attached to the Router

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

1. Select **BASIC > ReadySHARE**.

By default, the Basic radio button is selected, and the screen displays a USB storage device if it is attached to the router USB port.

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

2. (Optional) To view the files and folders on the USB device, click the network device name or the share name.

3. (Optional) To view more detail or to change the USB device settings, click the **Edit** button.

The USB Storage (Advanced Settings) screen displays. See *USB Storage Device Network and Access Settings* on page 51.

USB Storage Device Network and Access Settings

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

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

1. Select **ADVANCED > USB Storage > Advanced Settings**.

2. Specify access to the USB storage device.

- **Network Device Name**. The default is readyshare. This name is used to access the USB device that is connected to the 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**. Select the check boxes for the access methods that you want.
    - **Network Neighborhood/MacShare**. Enabled by default.
    - **HTTP**. Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB drive.
    - **HTTP (via Internet)**. Disabled by default. If you enable this feature, remote users can type **http://**<*public IP address/shares*> for example, http://1.1.10.102/shares) or a URL domain name to access the USB drive over the Internet. This feature supports file uploading only.
    - **FTP**. Disabled by default.
    - **FTP (via Internet)**. Disabled by default. If you enable this feature, remote users can access the USB drive through FTP over the Internet. This feature supports both downloading and uploading of files.

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

    Your changes are saved.

Available Network Folders

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

➢ **To view network folders:**

1. Select **ADVANCED > USB Storage > Advanced Settings**.

2. Scroll down to the Available Networks Folder section of the screen.

- **Share Name**. If only one device is connected, the default share name is USB_Storage. (Some router models have more than one USB port.)

  You can click the name, or you can type it in the address field of your web browser. If Not Shared is shown, the default share has been deleted, and no other share for the root folder exists. Click the link to change this setting.

- **Read Access and Write Access**. Show the permissions and access controls on the network folder: All – no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the router.

- **Folder Name**. Full path of the network folder.

- **Volume Name**. Volume name from the storage device (either USB drive or HDD).

- **Total Space and Free Space**. Show the current utilization of the storage device.

➢ **To add a network folder:**

1. Select **ADVANCED > ReadySHARE**.

2. Click the **Edit** button.

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

USB Device	U: (HP v100w)
Folder	U:\Photos\ Browse
Share Name	Vacation Photos
Read Access	All - no password
Write Access	All - no password

Apply

Close Window

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

4. In the Folder field, browse and select the folder.

5. Fill in the Share Name field.

6. In the Read Access list and the Write Access list, select the settings that you want.

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

7. Click the **Apply** button.

The folder is added on the USB device.

➢ **To edit a network folder:**

1. Select **ADVANCED > ReadySHARE**.

2. Click the **Edit** button.

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

3. Change the settings in the fields as needed.

4. Click the **Apply** button.

Your changes are saved.

Specify Approved USB Devices

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

➢ **To set up approved USB devices:**

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

2. Click the **Approved Devices** button.

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

3. In the Available USB Devices list, select the drive that you want to approve.

4. Click the **Add** button.

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

6. Click the **Apply** button.

Your change takes effect.

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

Media Server Settings

By default, the router acts as a ReadyDLNA media server, which lets you view movies and photos on DLNA/UPnP AV-compliant media players, such as Xbox360, Playstation, and NETGEAR media players.

➢ **To view these settings:**

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

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 router scans for media files whenever new files are added to the ReadySHARE USB hard drive.

2. Adjust the settings as needed:
   - **Enable Media Server**. Select this check box to enable this device to act as a media server.
   - **Enable TiVo support**. Select this check box if you want to play ReadyNAS media on your TiVo device. See the following section.
   - **Media Server Name**. Specify the name of the media server.
   - **Automatic (when new files added)**. Automatically scans for media files whenever new files are added to the ReadySHARE USB storage. Only shared folders with All – no password in The Read Access field can be scanned for media files.

3. Click the **Apply** button.

TiVo Support

You can set up your TiVo to access media files stored on a USB device that is connected to your router. The TiVo must be on the same network as the router. This feature supports the following file formats:

- **Video**. See and play mpeg1, and mpeg2 files.
- **Music**. See and play MP3 files.
- **Pictures**. View images in .jpg format.

Use ReadyDLNA to Play Media from Your Network on TiVo

You can use the TiVo (Series 2 and newer) Home Media Option to play photos and music on your Windows or Mac computer right in your TiVo user interface.

➢ **To set up the router to work with TiVo:**

1. Select **ADVANCED > USB Storage > Media Server**.
2. Make sure that the **Enable TiVo support** check box is selected.

➢ **To play videos:**

1. On the TiVo, select **TiVo Central > My Shows**.
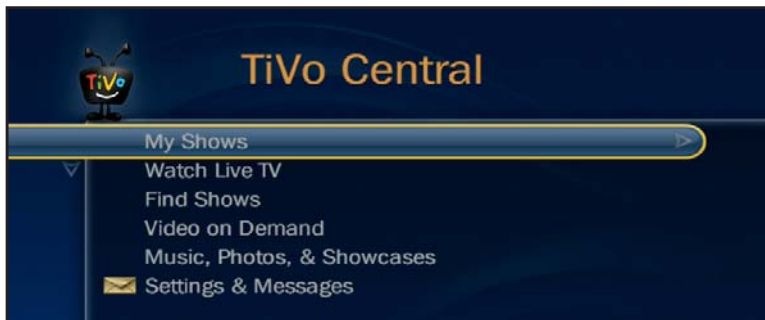
2. Go to the bottom of the list to find and select the R6200v2.

➢ **To play music or view photos:**

1. On the TiVo, select **TiVo Central > Music, Photos, & Showcases**.

2. Select what you want to play or watch.

➢ **To copy TiVo Files onto a computer:**

Use the TiVo Desktop accessory available at *https://www3.tivo.com/store/accessories-software.do*.
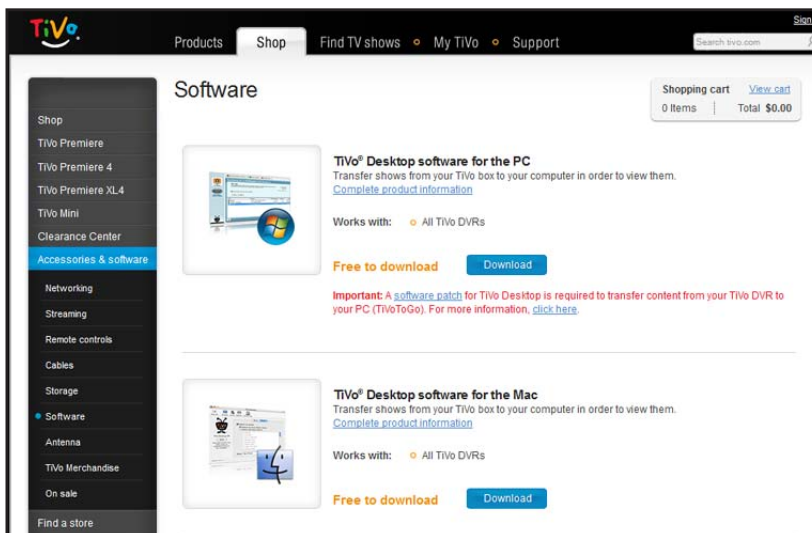
ReadySHARE Printer

6

Setting up and managing a shared USB printer

ReadySHARE Printer is compatible with Macs and Windows computers. It lets you connect a USB printer to the router USB port, and access it wirelessly.

This chapter contains the following sections:

- *ReadySHARE Printer Utility*
- *Set Up the ReadySHARE Printer Utility*
- *Install the NETGEAR USB Control Center*
- *Manage USB Print and Scan Jobs*

> **Note:** The USB port on the router can connect only to USB devices like flash drives, hard drives, and printers. Do not connect computers, USB modems, CD drives, or DVD drives to the router USB port.

ReadySHARE Printer Utility

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

You have to install this utility before you can use the ReadySHARE Printer feature.

- For this feature to work, this utility has to be installed and running in the background on each computer from which you want to control this USB printer.
- The driver software for the USB printer has to be installed on each computer from which you want to control this USB printer.
- The ReadySHARE Printer utility has both a Mac version and a Windows version.
- The ReadySHARE Printer utility setup file and instructions are available through this URL: *www.netgear.com/readyshare*

Once installed, the ReadySHARE Printer utility displays on your computer as the NETGEAR USB Control Center.

Set Up the ReadySHARE Printer Utility

You have to connect the USB printer to your router and install the utility on each computer in your network from which you want to control the USB printer.

➢ **To set up ReadySHARE Printer:**

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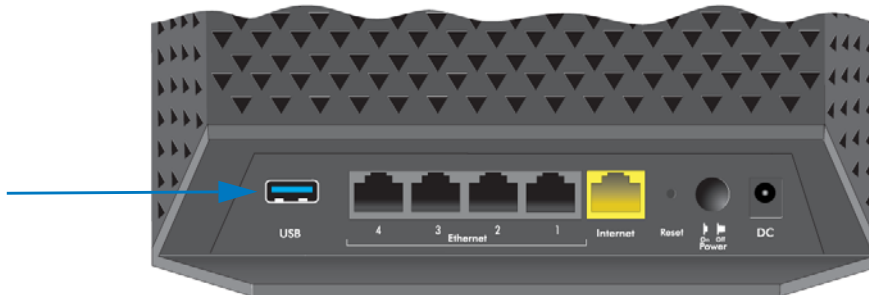
> **Note:** *Some USB printers (for example, HP and Lexmark printers) request that you do not connect the USB cable until the installation software prompts you.*

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

   If you do not have the printer driver, contact the printer manufacturer to find and download the most recent printer driver software.

3. Download the ReadySHARE Printer utility setup file and instructions from *www.netgear.com/readyshare*.

ReadySHARE® Printer

Wirelessly print from your home network to a connected USB printer

» **Easy to Set-up: Instructions**

» **PC Utility**

» **MAC Utility**

Supported Routers: WNDR4500, WNDR3800, WNDRMAC

4. On each computer on your network that shares the USB printer, install the ReadySHARE Printer utility.

Once installed, the ReadySHARE Printer utility displays on your computer as the NETGEAR USB Control Center.

Install the NETGEAR USB Control Center

For the ReadySHARE Print feature to work, this utility has to be installed and running in the background on each computer in the network from which you want to control this USB printer.

Once installed, the ReadySHARE Printer utility displays on your computers as the NETGEAR USB Control Center.

➢ **To install the NETGEAR USB Control Center:**

1. On each computer on your network that shares the USB printer, double-click the ReadySHARE Printer utility setup file that you downloaded.

The ReadySHARE Printer utility setup file and instructions can be downloaded through this URL: *www.netgear.com/readyshare.*

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

NETGEAR USB Control Center - InstallShield Wizard

Welcome to the InstallShield Wizard for NETGEAR USB Control Center

The InstallShield(R) Wizard will install NETGEAR USB Control Center on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

< Back   Next >   Cancel

3. Select the language and click the **OK** button.

The setup file installs the utility.

4. On each computer on your network that shares the USB printer, perform the initial setup of the NETGEAR USB Control Center.

    The first time you use the USB printer that is connected to your router, you are asked to select the USB printer. For more information, see the following section, *Set Up the NETGEAR USB Control Center*.

5. (Optional) Change the default settings.

    For more information, see *Configure the NETGEAR USB Control Center* on page 63.

Set Up the NETGEAR USB Control Center

The first time you access the utility, you are asked to select the printer.

*   When a USB printer is detected and connected automatically during the initial setup, you have to disconnect the printer and wait for the prompt asking you to click the Connect button.

*   You might be asked to install the driver for this printer. After the driver is installed, the printer status changes to Available.

➢ **To set up the NETGEAR USB Control Center:**

1. On each computer on your network that shares the USB printer, launch the NETGEAR USB Control Center the same way you launch any application program on your Windows or MAC computer.

2. Select the printer and click the **Connect** button.
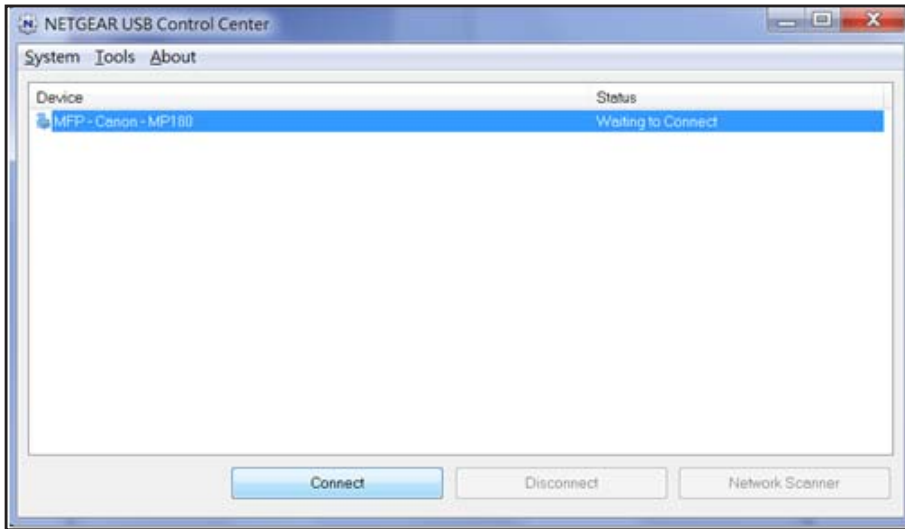
Once the connection is established, the status changes to Manually Connected by *xxx*.
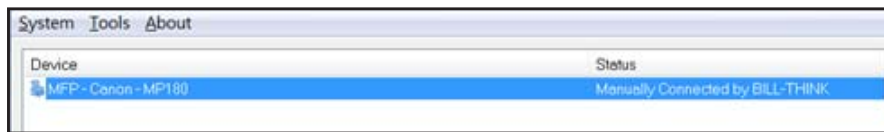
3. Click the **Disconnect** button.

The status changes to Available.
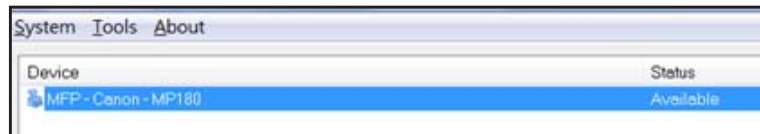
For each computer, after you click the Connect and Disconnect buttons once, the utility automatically handles the printing queue. The status of the printer appears as Available on all the computers.

The utility does not always need to hold the connection of a USB printer. After a print job is created for some USB printers, the NETGEAR USB Control Center connects to this USB printer automatically and prints. After the print job is done, the printer status might return to a Paused state.

For example, the USB printer displayed in the Windows Printers and Faxes window is ready for print jobs.
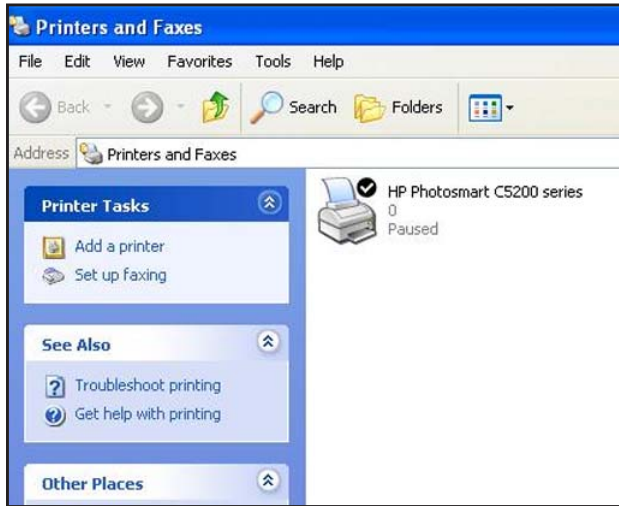
Configure the NETGEAR USB Control Center

You can set the time-out and specify other settings from the Control Center - Configuration screen.

➢ **To configure the NETGEAR USB Control Center:**

1. Launch the NETGEAR USB Control Center the same way you launch any application program on your Windows or MAC computer.

2. Select **Tools > Configuration**.

3. Specify the following settings:

   • **Automatically execute when logging on Windows**. Enable this utility to 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.

4. Click the **OK** button.

   Your changes are saved.

Manage USB Print and Scan Jobs

The NETGEAR USB Control Center utility runs in the background on each computer in your network. This utility manages the printing queue for the USB printer connected to your router.

After you activate the utility on each computer in the network, the status of the USB printer is Available on all of the computers.

- When the status is Available, you can use the USB printer from any computer in the network. The utility on each computer automatically manages the printing queue. The status of the USB printer appears as Available on all of the computers when no print jobs are in process.
- When the status is Manually Connected by xxx, only the xxx computer can use the printer. Other network devices must wait until the xxx computer has released the connection, or until the connection times out (the default time-out value is 30 seconds).

You can click the Disconnect button at any time to release the connection.

You can set the value for the default time-out time from the Configuration screen. For more information, see *Configure the NETGEAR USB Control Center* on page 63.

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

If your USB printer supports scanning, you can also use the USB printer for scanning. For more information, see *Use the Scan Feature of a Multifunction USB Printer* on page 65.

Launch the NETGEAR USB Control Center

The NETGEAR USB Control Center shows the availability status of the USB devices. The NETGEAR USB Control Center utility must be running for the computer to be able to print to the USB printer attached to the router. If you exit the utility, printing does not work.

➢ **To launch the NETGEAR USB Control Center:**

Launch the NETGEAR USB Control Center the same way you launch any application program on your Windows or MAC computer.
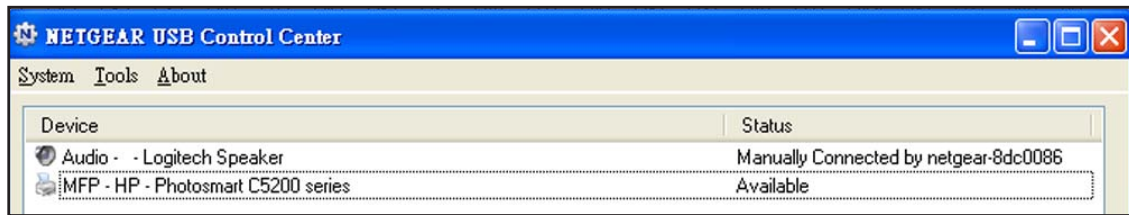
The main screen shows a device icon, the description for this USB device, and its status.

• **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. The first time you connect, you might be prompted to install the device driver.

The following menu selections display:

• **System**. Exit the utility.

• **Tools**. Access the Control Center - Configuration screen to set up your shared USB device. For more information, see *Configure the NETGEAR USB Control Center* on page 63.

• **About**. View details about the USB Control Center software.

The following control buttons are available:

• **Connect**. The first time you access the utility, you are asked to select the printer and click the Connect button.

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

• **Network Scanner**. This button activates the scanner window so that you can use the printer for scanning. Your printer must support scanning and be in the Available state.

Use the Scan Feature of a Multifunction USB Printer

If your USB printer supports scanning, you can also use the USB printer for scanning

➢ **To use the scan feature of a multifunction USB printer:**

1. Launch the NETGEAR USB Control Center the same way you launch any application program on your Windows or MAC computer.

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

3. Click the **Network Scanner** button.
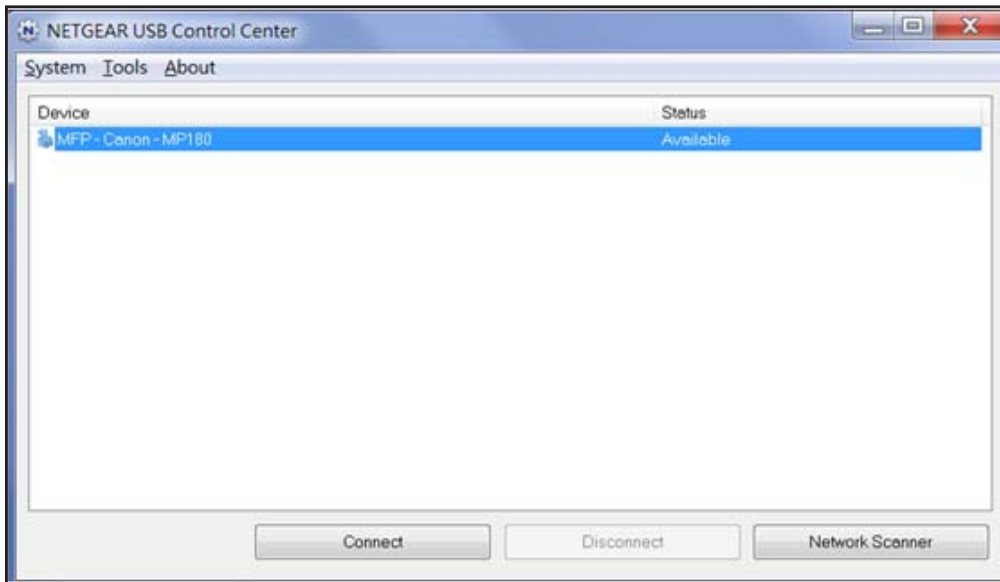
The scanner window opens so that you can use the USB printer for scanning.

Security 7

Customizing the firewall settings

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

This chapter includes the following sections:

- *Keyword Blocking of HTTP Traffic*
- *Block Services (Port Filtering)*
- *Port Triggering to Open Incoming Ports*
- *Port Forwarding to Permit External Host Communications*
- *How Port Forwarding Differs from Port Triggering*
- *Set Up Port Forwarding to Local Servers*
- *Set Up Port Triggering*
- *Schedule Blocking*
- *Set Up Security Event Email Notifications*

For information about Live Parental Controls, see *Parental Controls* on page 22.

Keyword Blocking of HTTP Traffic

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

➢ **To set up keyword blocking:**

1. Select **ADVANCED > Security > Block Sites**.
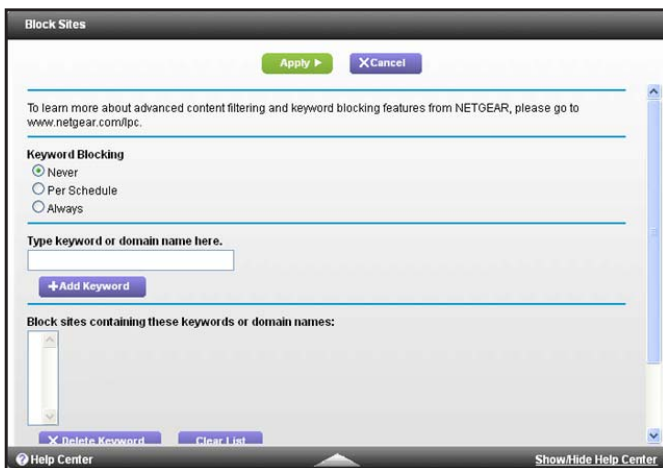
2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings. (See *Schedule Blocking* on page 77.)
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.

3. In the Keyword field, enter a keyword or domain, click the **Add Keyword** button.

4. Click the **Apply** button.

   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 the **Delete Keyword** button.

3. Click the **Apply** button.

   Your changes are saved.

➢ **To specify a trusted computer:**

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

1. In the Trusted IP Address field, enter the IP address.

2. Click the **Apply** button.

   Your changes are saved.

Block Services (Port Filtering)

Services are functions that server computers perform 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, a port number identifies the requested service. 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 Internet Engineering Task Force (IETF at *http://www.ietf.org/*) defines service numbers for many common protocols and they are 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 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 Block Services screen lets you add and block specific Internet services by computers on your network. This is called service blocking or port filtering. To add a service for blocking, first determine which port number or range of numbers the application uses.

➢ **To block services:**

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

2. Select either the **Per Schedule** or **Always** button.
3. If you selected Per Schedule, specify a time period in the Schedule screen.
4. Click the **Add** button to add a service.

The Block Services Setup screen displays:

5. From the Service Type list, select the application or service to allow or block.

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

6. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **TCP/UDP** (both).

7. Enter the starting and ending port numbers.

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

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

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

9. Click the **Add** button.

   Your changes are saved.

Port Triggering to Open Incoming Ports

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

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

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

1. You open an IRC client program to start a chat session on your computer.

2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

4. Noting your port triggering rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.

5. The IRC server sends a return message to your router using the NAT-assigned source port (for example, port 33333) as the destination port. The IRC server also sends an "identify" message to your router with destination port 113.

6. Upon receiving the incoming message to destination port 33333, your router checks its session table for an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.

7. Upon receiving the incoming message to destination port 113 your router checks its session table and finds an active session for port 113, associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.

8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or the relevant user groups or news groups.

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

Port Forwarding to Permit External Host Communications

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

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's

browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:

   - **Destination address**. The IP address of www.example.com, which is the address of your router.

   - **Destination port number**. 80, which is the standard port number for a web server process.

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

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

   The destination address is replaced with 192.168.1.123.

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

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your router.

4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

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

How Port Forwarding Differs from Port Triggering

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

- Any computer on your network can use port triggering, although only one computer can use it at a time.

- Port forwarding is configured for a single computer on your network.

- With port triggering, the router does not need to know the computer's IP address in advance. The IP address is captured automatically.

- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.

- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Set Up Port Forwarding to Local Servers

The port forwarding feature lets you allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding/Port Triggering screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before you start, determine which type of service, application, or game you want to provide, and the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

To ensure that your server computer always has the same IP address, use the reserved IP address feature of your product. See *Set Up Address Reservation* on page 38.

➢ **To forward specific incoming protocols:**

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

2. Leave the **Port Forwarding** radio button selected as the service type.
3. In the Service Name list, select the service name.
4. Click the **Add** button.

   A list of services displays. If the service that you want to add is not in the list, see *Add a Custom Service* on page 74.

5. Fill in the Server IP Address field.
6. Click the **Add** button.

   The service appears in the list on the Port Forwarding/Port Triggering screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, first determine which port number or range of numbers the application uses. You can usually determine this information by contacting the publisher of the application or user groups or news groups. When you have the port number information, follow these steps.

➢ **To add a custom service:**

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

2. Select the **Port Forwarding** radio button as the service type.

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

4. In the Service Name field, enter a descriptive name.

5. In the Service Type field, select the protocol. If you are unsure, select **TCP/UDP**.

6. In the External Starting Port field, enter the beginning port number.

   • If the application uses a single port, enter the same port number in the External Ending Port field.

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

7. Specify the internal ports by one of these methods:

   • Leave the **Use the same port range for Internal port** check box selected.

   • Fill in the Internal Starting Port and Internal Ending Port fields.

8. Click the **Apply** button.

   The service appears in the list in the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

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

2. Select the **Port Forwarding** radio button as the service type

3. In the table, select the radio button next to the service name.

4. Click the **Edit Service** or **Delete Service** button.

Application Example: Make a Local Web Server Public

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

➢ **To make a local web server public:**

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

   In this example, your router always gives your web server an IP address of 192.168.1.33.

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

   HTTP (port 80) is the standard protocol for web servers.

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

   To access your web server from the Internet, a remote user has to know the IP address that your ISP assigned. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Set Up Port Triggering

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

- More than one local computer needs port forwarding for the same application (but not simultaneously).

- An application needs to open incoming ports that are different from the outgoing port.

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

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

If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP). See *Universal Plug and Play* on page 104.

To configure port triggering, you need to know which inbound ports the application needs, and the number of the outbound port that will trigger the opening of the inbound ports. You

can usually determine this information by contacting the publisher of the application or user groups or news groups.

➢ **To enable port triggering:**

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

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

3. Clear the **Disable Port Triggering** check box.

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

---

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

This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. The time-out value is required so that the router can determine when the application has terminated.

➢ **To add a port triggering service:**

1. On the Port Forwarding/Port Triggering screen, click the **Add Service** button.

2. In the Service Name field, type a descriptive service name.

3. In the Service User list, select **Any,** or select **Single address** and enter the IP address of one computer.

    *   **Any** (the default), allows any computer on the Internet to use this service.

    *   **Single address** restricts the service to a particular computer.

4. Select the service type, either **TCP** or **UDP** or **TCP/UDP** (both). If you are not sure, select TCP/UDP.

5. In the Triggering Port field, enter the number of the outbound traffic port that will trigger the inbound ports to open.

6. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.

7. Click the **Apply** button.

    The service appears in the Port Triggering Portmap table.

8. Make sure that you enable port triggering so that the service that you added will be used.

Schedule Blocking

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

➢ **To schedule blocking:**

1. Select **ADVANCED > Security > Schedule**.

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 the **Every Day** check box to select the check boxes for all days.

    *   **Time of Day to Block**. Select a start and end time in 24-hour format, or select the **All Day** check box for 24-hour blocking.

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

4. Click the **Apply** button.

   Your settings are saved.

Set Up 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**.

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

3. In the Your Outgoing Mail Server field, enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com).

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

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

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

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. (Optional) Select the **Send Alerts Immediately** check box.

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

7. (Optional) Fill in the fields in the Send logs according to this schedule section of the screen.

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

8. Click the **Apply** button.

Your settings are saved.

Administration 8

Managing your network

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

This chapter includes the following sections:

- *Update the Router Firmware*
- *View Router Status*
- *View Logs*
- *Manage the Configuration File*
- *Change the Password*
- *Password Recovery*

For information about upgrading or checking the status of your router over the Internet, see *Remote Management* on page 103. For information about monitoring Internet traffic, see *Traffic Meter* on page 114.

Update the Router Firmware

The 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 Router Update screen to check if new firmware is available, and to update your product.

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

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

2. Click the **Check** button.

   The router finds new firmware information if it is available.

3. Click the **Yes** button.

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

⚠️ **WARNING:**

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

When the upload is complete, your router restarts. The upgrade process typically takes about 1oneminute. Read the new firmware release notes to find out if you need to reconfigure the router after upgrading.

View Router Status

➢ **To view router status and usage information:**

Select **Advanced Home** or select **Administration > Router Status**.

Router Information

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

Internet Port

- **MAC Address**. The Media Access Control address, which is the unique physical address used by the Internet (WAN) port of the router.
- **IP Address**. The IP address used by the Internet (WAN) port of the router. If no address is shown or the address is 0.0.0.0, the router cannot connect to the Internet.

- **Connection**. This shows if the router is using a fixed IP address on the WAN. If the value is DHCP Client, the router obtains an IP address dynamically from the ISP.
- **IP Subnet Mask**. The IP subnet mask used by the Internet (WAN) port of the router.
- **Domain Name Server**. The Domain Name Server addresses used by the router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.

Show Statistics Button

➢ **To view statistics:**

1. Select **Advanced Home** or select **Administration > Router Status**.

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

Show Statistics

System Up Time 00:07:00

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	1000M/Full	375	3572	0	325	3861	00:03:10
LAN1	Link Down						--
LAN2	1000M/Full	1809	1410	0	8714	744	00:03:10
LAN3	Link Down						--
LAN4	Link Down						--
2.4G WLAN b/g/n	217M	0	0	0	0	0	00:03:15
5G WLAN a/n/ac	867M	0	0	0	0	0	00:03:15

Poll Interval: 5   (5~86400 Seconds)   [Set Interval]   [Stop]

The following information is displayed:

- **System Up Time**. The time elapsed since the 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 the **Set Interval** button.

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

Connection Status Button

➢ **To view the Internet connection status:**

1. Select **Advanced Home** or select **Administration > Router Status**.

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

Connection Status	
IP Address	10.1.13.52
Subnet Mask	255.255.255.0
Default Gateway	10.1.13.13
DHCP Server	10.1.1.6
DNS Server	10.1.1.7 10.1.1.6
Lease Obtained	0 days,4 Hours,0 minutes
Lease Expires	0 days,3 Hours,56 minutes

Release   Renew

Close Window

The following information displays:

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

Click the **Release** button to return the status of all items to 0.

Click the **Renew** button to refresh the items.

Click the **Close Window** button to close the Connection Status screen.

Wireless Settings (2.4 GHz and 5 GHz)

The following settings are displayed:

- **Name (SSID)**. The wireless network name (SSID) that the router uses.

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

- **Channel**. The operating channel of the wireless port. The default channel at 2.4 GHz is Auto. When Auto is selected, the router finds the best channel available. For the 2.4 GHz setting, you can select channel 1 - 11 if your region is North America. In other regions, you can select channel 1-13.

  The default channel at 5 GHz is 53. For the 5 GHz setting, you can select channels 36, 40, 44, 48, 149, 157, and 161.

- **Mode**. The wireless communication mode. At 2.4 GHz, Up to 300 Mbps, Up to 145 Mbps, or Up to 54 Mbps. At 5 GHz, Up to 867 Mbps, Up to 400 Mbps, or Up to 173 Mbps.

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

- **Broadcast Name**. Indicates whether the router is broadcasting its SSID.

- **Wireless Isolation**. Wireless isolation prevents wireless clients from communicating with each other when they join the wireless network.

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

View Logs

The log is a detailed record of the websites you have accessed or attempted to access and other activities. 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.

➢ **To view logs:**

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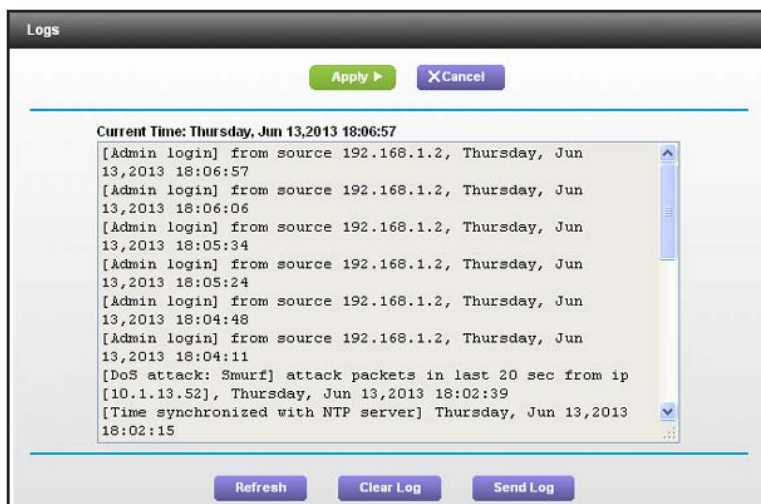
The Logs screen shows the following information:

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

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.

Manage the Configuration File

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

Back Up Settings

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

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

2. Click the **Backup Settings** button.
3. Specify a location to store the .cfg file.

   A copy of the current settings is saved.

Restore Configuration Settings

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

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

2. Click the **Browse** button and find the cfg file.

3. Click the **Restore** button.

   The files is uploaded to the router and the router reboots.

   ⚠️ **WARNING:**

   Do not interrupt the reboot process.

Erase the Current Configuration Settings

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

You can also use the Reset button on the back of the router to erase the configuration and restore the factory settings. (See *Factory Settings* on page 126.)

➢ **To erase the configuration settings:**

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

2. Click the **Erase** button.

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

Change the Password

This feature let you change the default password that is used to log in to the router with the user name **admin**. (For information about the WiFi password, see *Wireless Settings Screen Fields* on page 26.)

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

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

2. Type the old password, and type the new password twice.

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

4. Click the **Apply** button.

   Your changes take effect.

Password Recovery

NETGEAR recommends that you enable password recovery if you change the password for the router user name admin. Then you can recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➢ **To set up password recovery:**

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

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

3. Select two security questions, and provide answers to them.

4. Click the **Apply** button.

   Your changes are saved.

➢ **To recover your password:**

1. In the address field of your browser, type **www.routerlogin.net**.

   A login screen displays.

2. Click **Cancel**.

   If password recovery is enabled, you are prompted to answer two security questions.

3. Enter the saved answers to the security questions.

Advanced Settings

9

9.

Setting up unique situations

This chapter describes the advanced features of your router. Networking knowledge is needed to implement some of these features.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless Access Point*
- *Wireless Distribution System (WDS)*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*
- *IPv6*
- *Traffic Meter*

For information about approving a USB device, see *Specify Approved USB Devices* on page 54.

Advanced Wireless Settings

You can use this screen to turn the wireless radio on and off, to specify WPS settings, to use AP mode, and to set up a wireless access list.

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

Control the Wireless Radio

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

➢ **To turn the wireless radio on or off:**

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

   By default, the Enable Wireless Router Radio check box is selected.

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

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

3. (Optional) Select the **Turn off wireless signal by schedule** check box and fill in the fields to specify the times when you do not need a wireless connection.

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

4. Click the **Apply** button.

   Your changes take effect.

Set Up a Wireless Schedule

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

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

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

   The Advanced Wireless Settings screen displays.

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

3. Use the lists, radio buttons, and check boxes to set up a period during which you want to turn off the wireless signal.

4. Click the **Apply** button.

   The Advanced Wireless Settings screen displays.

5. Select the **Turn off wireless signal by schedule** check box to activate the schedule.

6. Click the **Apply** button.

View or Change WPS Settings

➢ **To specify WPS Settings:**

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

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

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

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

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

   By default, the Keep Existing Wireless Settings check box is selected. NETGEAR recommends that you leave this check box selected.

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

4. Click the **Apply** button.

   Your changes are saved.

Set Up a Wireless Access List by MAC Address

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

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

➢ **To restrict access based on MAC addresses:**

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

2. Click the **Set Up Access List** button.

3. Click the **Add** button.

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

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

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

   Tip: You can copy and paste the MAC addresses from the Attached Devices screen into the MAC Address field of this screen. To do this, use each wireless computer to join the wireless network. The computer should be listed in the Attached Devices screen.

5. Click the **Add** button.

    The screen changes back to the list screen.

6. Add each computer or device you want to allow to connect wirelessly.

7. Select the **Turn Access Control On** check box.

8. Click the **Apply** button.

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

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

    The Advanced Wireless Settings screen displays.

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

3. Do one of the following:
    • Click the **Edit** button.

      The Edit Wireless Card screen displays.

      a. Edit the address information.
      b. Click the **Accept** button.
    • Click the **Delete** button.

      The address is removed from the table.

Wireless Access Point

You can set up the router to run as an access point (AP) on the same local network as another router.

➢ **To set up the router as an AP:**

1. Use an Ethernet cable to connect the Internet port of this router to a LAN port in the other router.
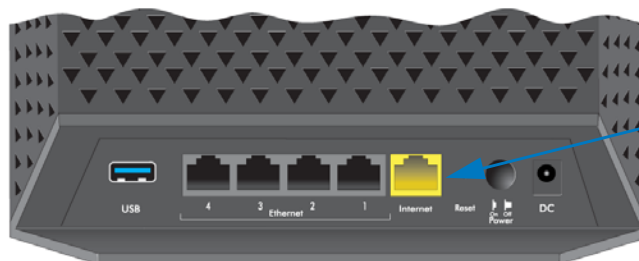
Cable this port to a LAN port on the other router

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

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

The AP Mode section of the screen expands.
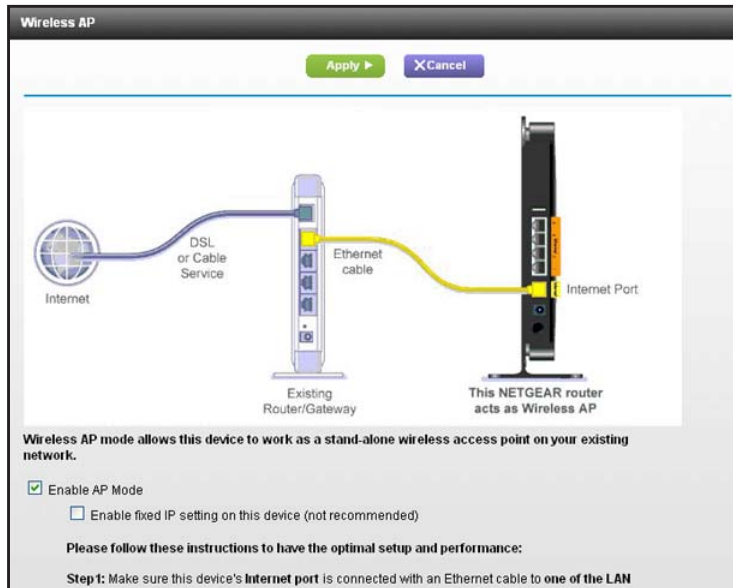
4. Select a check box for one of the following IP address settings:
    *   **Get an IP address dynamically from the other router**. The other router on the network assigns an IP address to this router while this router is in AP mode.
    *   **Fixed IP address (not recommended)**. Use this setting if you want to manually assign a specific IP address to this router while it is in AP mode. Using this option effectively requires advanced network experience.

    Note: *To avoid interference, NETGEAR recommends that you use different wireless settings for the router in access point mode. You could also turn off the wireless radio on the other router or gateway and use your router only for wireless client access.*

5. Click the **Apply** button.

    The IP address of the router changes, and you are disconnected. To reconnect, close and restart your web browser, and type **http://www.routerlogin.net**.

Set Up the Router in Bridge Mode

You can use your R6200v2 Smart WiFi Router in bridge mode to connect multiple devices wirelessly at the faster 802.11ac speed. To do this, you need two routers: one set up as a router and the other set up as a bridge.

R6200v2 Smart WiFi Router	R6200v2 Smart WiFi Router in bridge mode
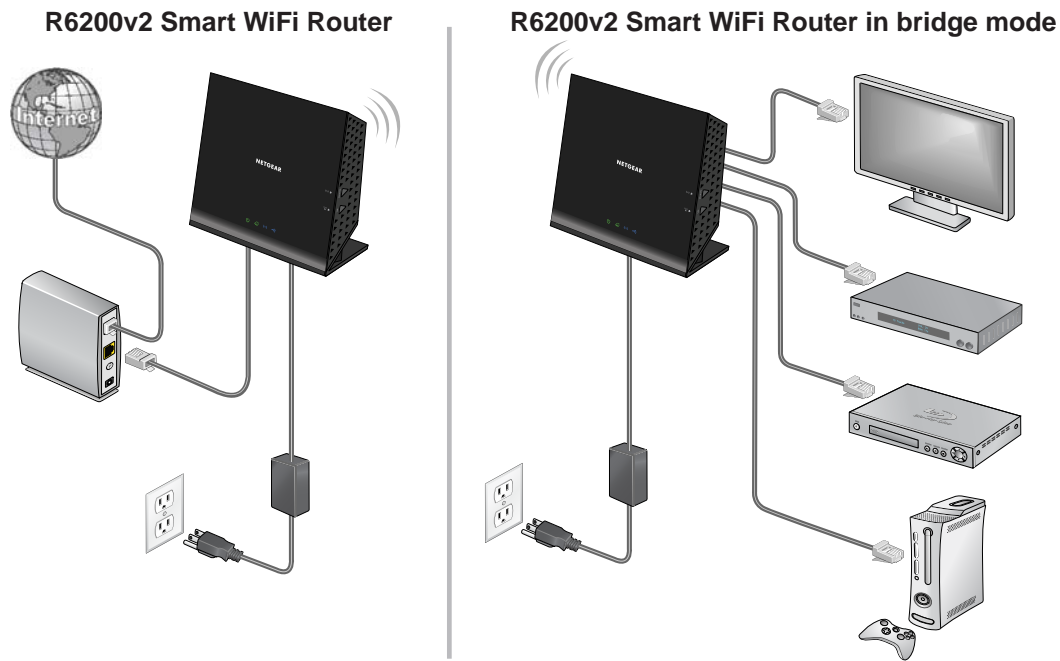
Figure 8. Router in bridge mode with an 802.11ac WiFi connection

Installing your router as a bridge offers the following benefits:

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

For example, you could install the first router in a room like a home office that has your Internet connection. Then set up the second router in bridge mode. Then place the router in Bridge mode in a different room that has your home entertainment center. Cable the router in Bridge mode to your Smart TV, DVR, game console or Blu-ray player, and use its 802.11ac WiFi connection to the first router.

➢ **To set up Bridge mode:**

1. Make a note of the WiFi settings of the other router to which this router will connect:

   You need to know the SSID, WiFi security mode, wireless password, and operating frequency (either 2.4 GHz or 5 GHz).

2. On the router that will run in Bridge mode, select **ADVANCED > Advanced Setup > Wireless Settings**.

3. Scroll down and select the **Use other operation mode** check box and the **Enable Bridge mode** radio button.

   The screen adjusts.
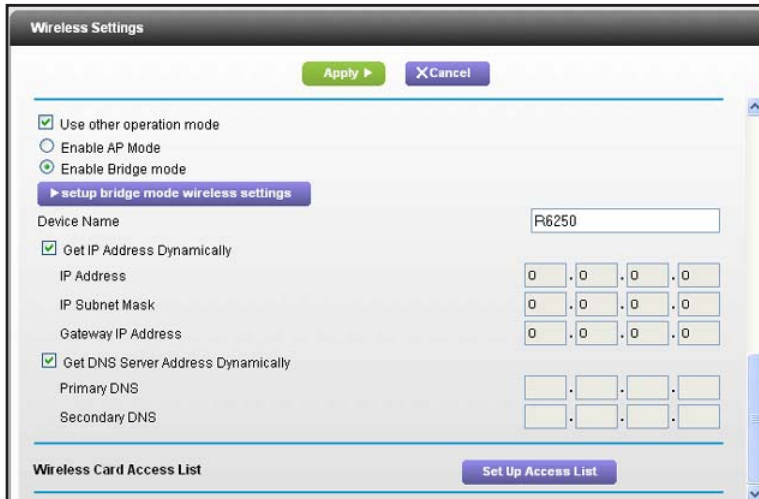
4. Click the **setup bridge mode wireless settings** button.
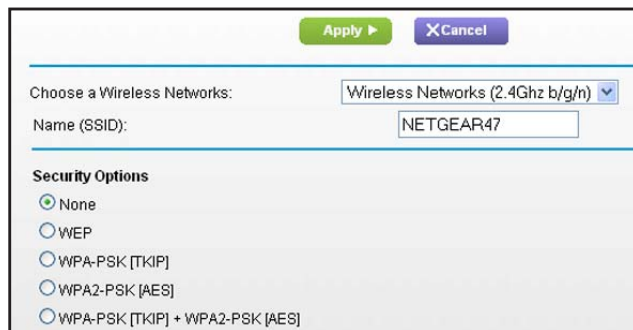
5. Specify the settings of the other router to which this router will connect.

   a. Select the wireless network frequency (2.4 GHz or 5 GHz).

      For 802.11ac mode, select 5 GHz.

   b. In the Name (SSID) field, enter the wireless network name (SSID).

   c. In the Security Option section, select a radio button.

   d. If prompted, type the passphrase (the WiFi password that you use to connect to the other router).

6. Click the **Apply** button.

   The settings for the other router are saved and the Advanced Wireless Settings screen displays.

7. Click the **Apply** button on the Advanced Wireless Settings screen.

   Your changes take effect.

Wireless Distribution System (WDS)

You can set the router up to be used as a wireless base station or a wireless repeater in a wireless distribution system (WDS). A WDS lets you expand a wireless network through multiple access points. A wireless base station connects to the Internet, can have wired and wireless clients, and sends its wireless signal to an access point that functions as a wireless repeater. A wireless repeater can also have wired and wireless clients, but connects to the Internet through the wireless base station. The following figure shows a wireless repeating scenario.
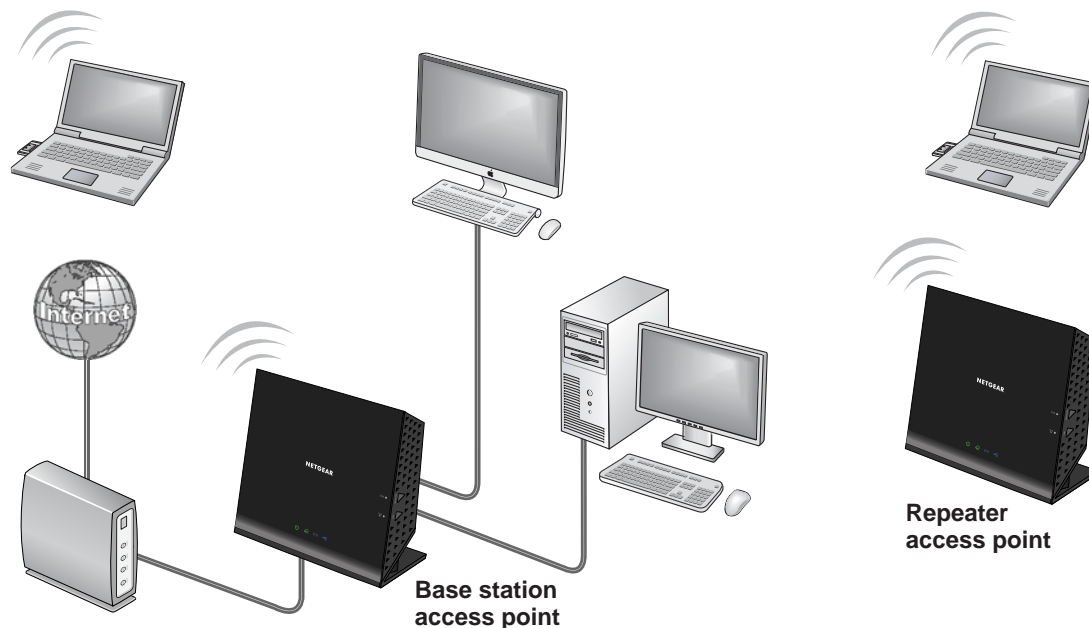
Figure 9. Wireless repeating scenario

Note: To use the wireless repeating function, you need to select None as the security option in the Wireless Settings screen, and you cannot select Auto Channel.

Wireless base station. The router acts as the parent access point that bridges traffic to and from the child repeater access point. The base station also handles wireless and wired local computers. To configure this mode, you have to know the MAC addresses of the child repeater access point. Often, the MAC address is on the product label.

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

The router is always in dual-band concurrent mode, unless you turn off one radio. If you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base

---

station in either radio band and use the other radio band as a wireless router or wireless base station, dual-band concurrent mode is not affected.

For you to set up a wireless network with WDS, both access points have to meet the following conditions:

• Both access points have to use the same SSID, wireless channel, and encryption mode.

• Both access points have to be on the same LAN IP subnet. That is, all of the access point LAN IP addresses are in the same network.

• All LAN devices (wired and wireless computers) are configured to operate in the same LAN network address range as the access points.

Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to know the MAC address of the remote unit. First, set up the base station. Then set up the repeater.

➤ **To set up the base station:**

1. Set up both units with the same wireless settings.

    The SSID and mode need to be the same and the wireless security option has to be set to None. (See *Basic Wireless Settings* on page 25.)

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

3. Select the **Enable Wireless Repeating Function** check box.

4. Select the **Wireless Base Station** radio button.

5. (Optional) Select the **Disable Wireless Client Association** check box to prevent wireless clients from associating with the base station and allow LAN client associations only.

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

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

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

7. Click the **Apply** button.

   Your changes are saved.

Set Up a Repeater

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

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

➢ **To configure the router as a repeater:**

1. Log in to the router that will be the repeater.

2. Select **BASIC > Wireless Settings** and verify that the wireless settings match the base unit exactly.

   The wireless security option has to be set to **WEP** or **None**.

3. Select **ADVANCED > Wireless Repeating Function**.

4. Select the **Enable Wireless Repeating Function** check box.

5. Select the **Wireless Repeater** radio button.

6. Fill in the Repeater IP Address field.

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

7. (Optional) Select the **Disable Wireless Client Association** check box to prevent wireless clients from associating with the repeater and allowing LAN client associations only.

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

8. In the Base Station MAC Address field, enter the MAC addresses for the access point that should function as the base station.

9. Click the **Apply** button.

   Your changes are saved.

10. Verify connectivity across the LANs.

    A computer on any wireless or wired LAN segment of the router can connect to the Internet or share files and printers with any other computer or server connected to the other access point.

Dynamic DNS

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

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

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

➢ **To set up Dynamic DNS:**

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

2. Register for an account with one of the Dynamic DNS service providers whose URLs are in the Service Provider list.

3. Select the **Use a Dynamic DNS Service** check box.

4. Select the URL of your Dynamic DNS service provider.

   For example, for DynDNS.org, select **www.dyndns.org**.

5. Type the host name (or domain name) that your Dynamic DNS service provider gave you.

6. Type the user name for your Dynamic DNS account.

   This user name is the name that you use to log in to your account, not your host name.

7. Type the password (or key) for your Dynamic DNS account.

8. Click the **Apply** button.

   Your changes are saved.

Static Routes

Static routes provide more routing information to your router. Typically, you do not need to add static routes. You have to configure static routes only for unusual cases such as multiple routers or multiple IP subnets on your network.

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

- Your primary Internet access is through a cable modem to an ISP.

- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.

- Your company's network address is 134.177.0.0.

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

Advanced Settings

101

In this case you have to define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.

- The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.1.100.

- A metric value of 1 works because the ISDN router is on the LAN.

- Private is selected only as a precautionary security measure in case RIP is activated.

➢ **To set up a static route:**

1. Select **ADVANCED > Advanced Setup > Static Routes**.
2. Click **Add**.

3. In the Route Name field, type a name for this static route (for identification purposes only.)
4. Select the **Private** check box if you want to limit access to the LAN only.

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

5. Select the **Active** check box to make this route effective.
6. Type the IP address of the final destination.
7. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
8. Type the gateway IP address, which has to be on the same LAN segment as the router.
9. Type a number from 1 through 15 as the metric value.

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

10. Click the **Apply** button.

   The static route is added.

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

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

   The Static Routes screen displays.

2. In the table, select the radio button next to the route that you want to edit or delete.
3. Do one of the following:

- Click the **Edit** button.

  The Static Routes screen adjusts.

  a. Edit the route information.

  b. Click the **Apply** button.

- Click the **Delete** button.

  The route is removed from the table.

Remote Management

The remote management feature lets you access your router over the Internet to view or change its settings.

Note: Be sure to change the router default login password to a secure password. The ideal password contains no dictionary words from any language and contains uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters. See *Change the Password* on page 87.

➢ **To set up remote management:**

1. Select **ADVANCED > Advanced Setup > Remote Management**.

2. Select the **Turn Remote Management On** check box.

3. Under Allow Remote Access By, specify the external IP addresses to be allowed to access the router's remote management.

   Note: *For enhanced security, restrict access to as few external IP addresses as practical.*

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.

- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address for the allowed range.

- To specify IP addresses, select **IP Address List** and type in the allowed IP addresses.

- To allow access from any IP address on the Internet, select **Everyone**.

4. Specify the port number for accessing the web management interface.

   Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click the **Apply** button.

   Your changes take effect.

6. When you access your router from the Internet, type your router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number.

   For example, if your external address is 134.177.0.123 and you use port number 8080, enter **http://134.177.0.123:8080** in your browser.

Universal Plug and Play

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

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.

➢ **To turn on Universal Plug and Play:**

1. Select **ADVANCED > Advanced Setup > UPnP**.

   The UPnP screen displays.

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

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

3. Type the advertisement period in minutes.

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

4. Type the advertisement time to live in hops.

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

5. Click the **Apply** button.

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

6. (Optional) To refresh the information in the UPnP Portmap table, click the **Refresh** button.

IPv6

You can use this feature to set up an IPv6 Internet connection type if genie does not detect it automatically.

➢ **To set up an IPv6 Internet connection type:**

1. Select **ADVANCED > Advanced Setup > IPv6**.
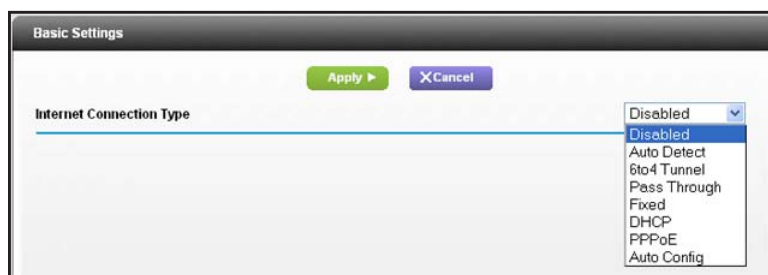
2. In the Internet Connection Type list, select the IPv6 connection type.

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

- If your ISP did not provide details, you can select **IPv6 Tunnel**.

- If you are not sure, select **Auto Detect** so that the router detects the IPv6 type that is in use.

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

For more information about Internet connection types, see the following sections.

3. Click the **Apply** button.

   Your changes take effect.

Requirements for Entering IPv6 Addresses

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted.

The following errors invalidate an IPv6 address:

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

Auto Detect

➢ **To set up an IPv6 Internet connection through auto detection:**

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

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **Auto Detect**.

   The screen adjusts:

The router automatically detects the information in the following fields:

- **Connection Type**. This field indicates the connection type that is detected.

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

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

3. Specify how the router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:

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

   - **Auto Config**. This is the default setting.

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

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

5. Click the **Apply** button.

IPv6 Auto Config

➢ **To set up an IPv6 Internet connection through auto configuration:**

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

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **Auto Config**.

   The screen adjusts:

The router automatically detects the information in the following fields:

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

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

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

   Most people do not need to fill in this field, but if your ISP has given you a specific host name, enter it here.

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

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

5. Specify how the router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:

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

   - **Auto Config**. This is the default setting.

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

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

7. Click the **Apply** button.

IPv6 6to4 Tunnel

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

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

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

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **6to4 Tunnel**.

The screen adjusts:

The router automatically detects the information in the following fields:

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

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

3. Configure the remote 6to4 relay router settings by selecting one of the following buttons:

- **Auto**. Your router uses any remote relay router that is available on the Internet. This is the default setting.

- **Static IP Address**. Enter the static IPv4 address of the remote relay router. This address is usually provided by your IPv6 ISP.

4. Specify how the router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:

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

- **Auto Config**. This is the default setting.

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

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

6. Click the **Apply** button.

IPv6 Pass Through

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

➢ **To set up a pass-through IPv6 Internet connection:**

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

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **Pass Through**.

   The screen adjusts, but no additional fields display.

3. Click the **Apply** button.

IPv6 Fixed

➢ **To set up a fixed IPv6 Internet connection:**

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

   The IPv6 screen displays.

2. Select **Fixed** from the menu.

   The screen adjusts:

3. Configure the fixed IPv6 addresses for the WAN connection:

   • **IPv6 Address/Prefix Length**. The IPv6 address and prefix length of the router WAN interface.

   • **Default IPv6 Gateway**. The IPv6 address of the default IPv6 gateway for the router's WAN interface.

   • **Primary DNS Server**. The primary DNS server that resolves IPv6 domain name records for the router.

   • **Secondary DNS Server**. The secondary DNS server that resolves IPv6 domain name records for the router.

> **Note:** *If you do not specify the DNS servers, the router uses the DNS servers that are configured for the IPv4 Internet connection on the Internet Setup screen. (See Internet Setup on page 20.)*

4. Specify how the router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:

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

5. In the IPv6 Address/Prefix Length fields, specify the static IPv6 address and prefix length of the router's LAN interface.

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

6. Click the **Apply** button.

IPv6 DHCP

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

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

    The IPv6 screen displays.

2. In the Internet Connection Type list, select **DHCP**.

    The screen adjusts:

The router automatically detects the information in the following fields:

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

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

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

   Most people do not need to fill in this field, but if your ISP has given you a specific host name, enter it here.

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

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

5. Specify how the router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:

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

   - **Auto Config**. This is the default setting.

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

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

7. Click the **Apply** button.

IPv6 PPPoE

➤ **To set up a PPPoE IPv6 Internet connection:**

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

   The IPv6 screen displays.

2. In the Internet Connection Type list, select **PPPoE**.

The screen adjusts:

The router automatically detects the information in the following fields:

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

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

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

   This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, then you would type JerAB in this field. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, type it in this field.

4. In the Password field, enter the password for the ISP connection.

5. In the Service Name name field, enter a service name.

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

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

6. Specify how the router assigns IPv6 addresses to the devices on your home network (the LAN) by selecting one of the following radio buttons:

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

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

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

8. Click the **Apply** button.

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic that passes through the router Internet port. You can set limits for traffic volume.

➢ **To monitor Internet traffic:**

1. Click **ADVANCED > Advanced Setup > Traffic Meter**.

Scroll to view more settings

2. Select the **Enable Traffic Meter** check box.
3. (Optional) Control the volume of Internet traffic.

   You can use either the traffic volume control feature or the connection time control feature.

   - Select the **Traffic volume control by** radio button and then select one of the following options:
     - **No Limit**. No restriction is applied when the traffic limit is reached.
     - **Download only**. The restriction is applied to incoming traffic only.
     - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
   - Select the **Connection time control** radio button and enter the allowed hours in the Monthly limit field.

4. (Optional) If your ISP charges for extra data volume when you make a new connection, enter the extra data volume in MB in the Round up data volume for each connection by field.

5. In the Traffic Counter section, set the traffic counter to begin at a specific time and date.

   If you want the traffic counter to start immediately, click the **Restart Counter Now** button.

6. In the Traffic Control section, specify whether the router should issue a warning message before the monthly limit of Mbytes or hours is reached.

   By default, the value is 0 and no warning message is issued. You can select one of the following to occur when the limit is attained:

   • The Internet LED flashes green or amber.

   • The Internet connection is disconnected and disabled.

7. Click the **Apply** button.

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

Click the **Refresh** button to update the Traffic Statistics section.

Click the **Traffic Status** button to display more information about the data traffic on your router and to change the poll interval.

Troubleshooting 10

This chapter provides information to help you diagnose and solve problems you might have with your router. If you do not find the solution here, check the NETGEAR support site at *http://support.netgear.com* for product and contact information.

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshoot with the LEDs*
- *Cannot Log In to the Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *Wireless Connectivity*
- *Troubleshoot Your Network Using the Ping Utility*

Quick Tips

This section describes tips for troubleshooting some common problems.

Sequence to Restart Your Network

When you need to restart your network, follow this sequence:

1. Turn off *and* unplug the modem.
2. Turn off the router.
3. Plug in the modem and turn it on. Wait 2 minutes.
4. Turn on the router and wait 2 minutes.

Check Ethernet Cable Connections

If your device does not power on, make sure that the Ethernet cables are securely plugged in.

- The Internet LED on the router is on if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.
- For each powered-on computer connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED is on.

Wireless Settings

Make sure that the wireless settings in the computer and router match exactly.

- For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer need to match exactly.
- If you set up an access list in the Advanced Wireless Settings screen, you have to add each wireless computer's MAC address to the router's access list.

Network Settings

Make sure that the network settings of the computer are correct.

- Wired and wirelessly connected computers need to have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen.

Troubleshoot with the LEDs

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power/Test LED ⏻ is lit.
2. Verify that the Power/Test LED turns amber within a few seconds, indicating that the self-test is running.
3. After approximately 30 seconds, verify the following:
   - The Power/Test LED is solid green.
   - The Internet LED is lit.
   - The Wireless LED is lit unless you turned off the wireless radio.

The LEDs on the front panel of the router can be used for troubleshooting.

Power/Test LED Is Off or Blinking

- Make sure that the power cord is securely connected to your router and that the power adapter is securely connected to a functioning power outlet.
- Check that you are using the 12V DC, 2.5A power adapter that NETGEAR supplied for this product.
- If the Power/Test LED blinks slowly and continuously, the router firmware is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. If the error persists, you have a hardware problem. For recovery instructions, or help with a hardware problem, contact technical support at *www.netgear.com/support.*

Power LED Stays Amber

When the router is turned on, the Power LED lights amber for about 20 seconds and then lights green. If the LED does not light green, the router has a problem.

If the Power LED is lit amber 1 minute after you turn on power to the router:

1. Turn off the power and then turn it back on to see if the router recovers.
2. Press and hold the **Reset** button.

   The router returns to its factory settings.

   See *Troubleshoot Your Network Using the Ping Utility* on page 123.

If the error persists, you might have a hardware problem. Contact technical support at *www.netgear.com/support.*

LEDs Never Turn Off

When the router is turned on, if all LEDs are still lit 1 minute after power-up:

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

  The router returns to its factory settings. For more information, see *Troubleshoot Your Network Using the Ping Utility* on page 123.

If the error persists, you might have a hardware problem. Contact technical support at *www.netgear.com/support*.

Internet LEDs Is Off

If the Internet LED does not light when the router has power, check the following:

- Make sure that the cable connections are secure at the router and at the modem.
- Make sure that power is turned on to the connected modem.
- Be sure that you are using the correct cable.

  When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem.

WiFi LED Is Off

If the Wireless LED stays off, check to see if the WiFi On/Off button on the router has been pressed. This button turns the wireless radio in the router on and off. The Wireless LED lights when the wireless radio is turned on.

Cannot Log In to the Router

If you are unable to log in to the router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The login name is **admin**, and the default password is **password**. Make sure that Caps Lock is off when you enter this information.
- If you are attempting to set up your router and there is another router in your network, make sure that you are using Bridge Mode. See *Set Up the Router in Bridge Mode* on page 95.

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

- If you specify IP addresses in your network:
  - Make sure that the IP address of your computer is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254.

  - If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.

  - If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to its factory settings. This sets the router's IP address to 192.168.1.1. For more information, see *Factory Settings* on page 126.

Cannot Access the Internet

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

➢ **To check the WAN IP address:**

1. Start your browser, and select an external site such as *www.netgear.com*.

2. Access the router interface at **www.routerlogin.net**.

3. Select **Administration > Router Status**.

4. Check that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network. For more information, see *Sequence to Restart Your Network* on page 117.

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

- Your Internet service provider (ISP) might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.

- If your ISP requires a login, the login name and password might be set incorrectly.

- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Internet Setup screen.

- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case, do one of the following:

    - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

    - Configure your router to clone your computer's MAC address.

If your router can obtain an IP address, but your computer is unable to load any web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

    A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer, and verify the DNS address. You can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the router configured as its TCP/IP gateway.

    If your computer obtains its information from the router by DHCP, reboot the computer, and verify the gateway address.

- You might be running login software that is no longer needed.

    If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**.

Troubleshoot PPPoE

If you are using PPPoE, try troubleshooting your Internet connection.

➢ **To troubleshoot a PPPoE connection:**

1. Select **Administration > Router Status**.
2. Click **Connection Status**.
3. Check the Connection Status display to see if your PPPoE connection is up and working.
4. If any of the fields on the Connection Status screen indicate Failed, you can attempt to reconnect by clicking **Connect**. The router continues to attempt to connect indefinitely.
5. If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There might also be a provisioning problem with your ISP.

Note: Unless you connect manually, the router does not authenticate using PPPoE until data is transmitted to the network.

Troubleshoot Internet Browsing

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet, check the following:

*   Your computer might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.

    Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, restart your computer.

    Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

*   Your computer might not have the router configured as its default gateway.

    Reboot the computer and verify that the router address (www.routerlogin.net) is listed by your computer as the default gateway address.

*   You might be running login software that is no longer needed. If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**.

Changes Not Saved

If the router does not save the changes you make in the router interface, check the following:

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

Wireless Connectivity

If you are having trouble connecting wirelessly to the router, try to isolate the problem.

*   Does the wireless device or computer that you are using find your wireless network?

    If not, check the WiFi LED on the front of the router. If it is off, you can press the **WiFi On/Off** button on the side of the router to turn the router wireless radios back on.

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

*   Does your wireless device support the security that you are using for your wireless network (WPA or WPA2)?

- If you want to view the wireless settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, and select **Wireless** see (*Basic Wireless Settings* on page 25).

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

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

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

Troubleshoot Your Network Using the Ping Utility

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

Test the LAN Path to Your Router

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

➢ **To ping the router from a Windows computer:**

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

   ping www.routerlogin.net

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address > with 32 bytes of data
   ```

   If the path is working, you see this message:

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

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

   ```
   Request timed out
   ```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections

   For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.

Check that the appropriate LEDs are on for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and router.

- Wrong network configuration

Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the Windows Run window, type:

   ping -n 10 *<IP address>*

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

If the path is functioning correctly, replies like those shown in the previous section are displayed.

If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Internet Setup screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers.

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

Supplemental Information

A

This appendix covers the following topics:

- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can return the router to its factory settings. Use the end of a paper clip or a similar object to press and hold the **Reset** button on the back of the router for at least 7 seconds. The router resets, and returns to the factory configuration settings shown in the following table.

Table 3. Factory default settings

Feature		Default behavior
Router login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	AutoSensing
Local network (LAN)	LAN IP	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	Pacific time
	Time zone daylight savings time	Disabled
	Allow a registrar to configure this router	Enabled
	DHCP starting IP address	192.168.1.2
	DHCP ending IP address	192.168.1.254
	DMZ	Disabled
	Time zone	GMT for WW except NA and GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Table 3. Factory default settings (continued)

Feature		Default behavior
Wireless	Wireless communication	Enabled
	SSID name	See router label
	Security	WPA2-PSK (AES)
	Broadcast SSID	Enabled
	Transmission speed	Auto[*]
	Country/region	United States in the US; otherwise varies by region
	RF channel	6 until region selected
	Operating mode	Up to 145 Mbps at 2.4 GHz, Up to 867 Mbps at 5 GHz
Firewall	Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests)
	Outbound (communications going out to the Internet)	Enabled (all)

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

Technical Specifications

Table 4. R6200v2 Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power adapter	• North America: 120V, 60 Hz, input • UK, Australia: 240V, 50 Hz, input • Europe: 230V, 50 Hz, input • All regions (output): 12V DC @ 2.5A, output
Dimensions	Dimensions: 1195 x 199 x 65 mm (7.68 x 7.83 x 2.56 in.)
Weight	Weight: 417g (0.91 lbs)
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	FCC Part 15 Class B VCCI Class B EN 55 022 (CISPR 22), Class B C-Tick N10947
LAN	10BASE-T or 100BASE-Tx or 1000BASE-T, RJ-45
WAN	10BASE-T or 100BASE-Tx or 1000BASE-T, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for the previous table.
Radio data rates	Auto Rate Sensing
Data encoding standards	IEEE 802.11ac 2.0 IEEE 802.11n version 2.0 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b 2.4 GHz IEEE 802.11n, IEEE 802.11a 5.0 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).

Operating frequency range	2.4 GHz
	    2.412–2.462 GHz (US)
	    2.412–2.472 GHz (Japan)
	    2.412–2.472 GHz (Europe ETSI)
	5 GHz
	    5.18–5.24 + 5.745–5.825 GHz (US)
	    5.18–5.24 GHz (Europe ETSI)

802.11 security	WPA-PSK, WPA2-PSK, and WPA/WPA2

Notification of Compliance

NETGEAR Dual Band - Wireless

B

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Products bearing the CE marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

Intended for indoor use only in all EU member states, EFTA states, and Switzerland.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the R6200v2 Smart WiFi Router complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.
- All cables used to connect peripherals must be shielded and grounded. Operation with cables connected to peripherals that are not sheilded and grounded may result interference to radio and television reception.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (R6200v2 Smart WiFi Router) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce po-tential for harmful interference to co-channel mobile satellite systems.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utili-sation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Interference Reduction Table

The following table shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters