LTE Broadband 11n Wireless Router MBR1515

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

November 2012
202-11102-01
v1.0

Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the support website at *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 1 Hardware Setup

Chapter 2 Getting Started with NETGEAR genie

Chapter 3 NETGEAR genie BASIC Settings

Chapter 4 NETGEAR genie ADVANCED Home

Chapter 5 Security

Chapter 6 Administration

Chapter 7 Advanced Settings

Chapter 8 Troubleshooting

Appendix A Supplemental Information

Appendix B Wall-Mounting

Appendix C Notification of Compliance

Index

1 Hardware Setup

Getting to know your router

The LTE Broadband 11n Wireless Router MBR1515 provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over the high-speed Verizon 4G LTE wireless network. It lets you block unsafe Internet content and applications and protects the devices (computers, gaming consoles, and so on) that you connect to your home network.

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

This chapter contains the following sections:

- *Hardware Features*
- *Insert the SIM Card*
- *Position Your Router*

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

Hardware Features

This section outlines the physical aspects of your router.

Position your router upright. Place the router near an AC power outlet in a location where you can connect the cables you need for your home network. The router must also be located where you can receive a strong mobile broadband signal while indoors if you are planning to connect to the Internet using mobile broadband.

Router Front Panel

The router front panel contains control buttons and status LEDs. Use the LEDs to verify status and connections.

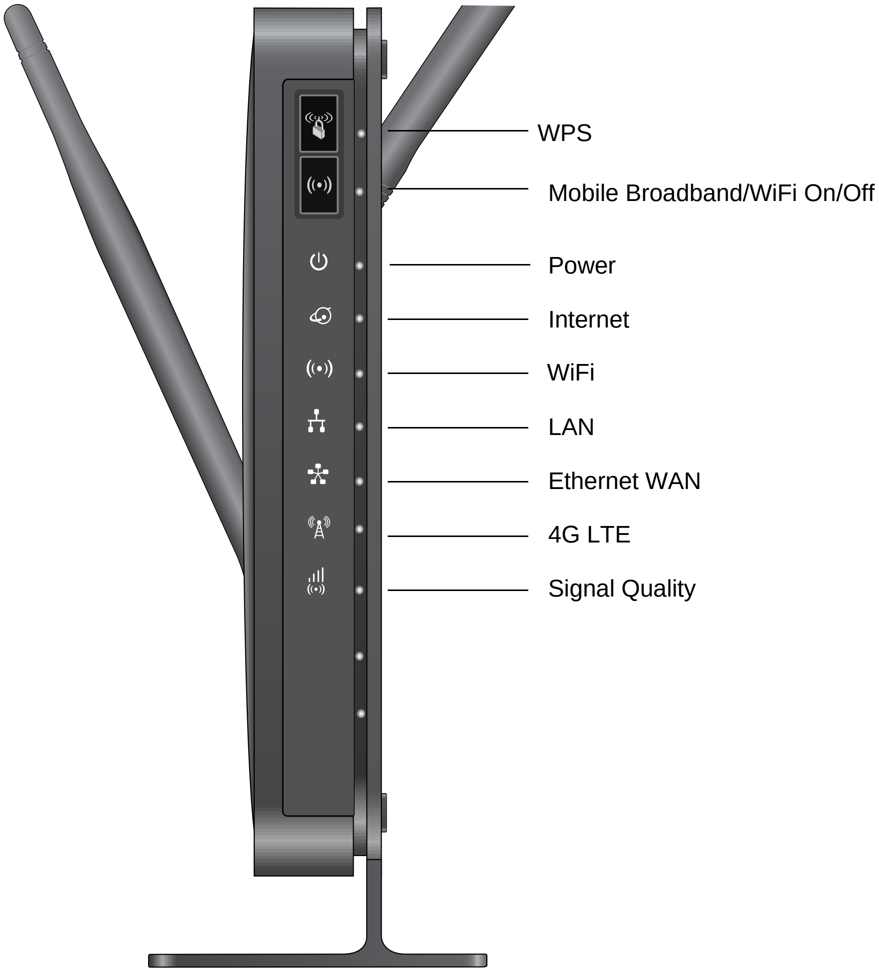
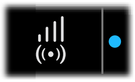


Table 1 describes each LED and button on the front panel of the router.

Table 1. LED descriptions

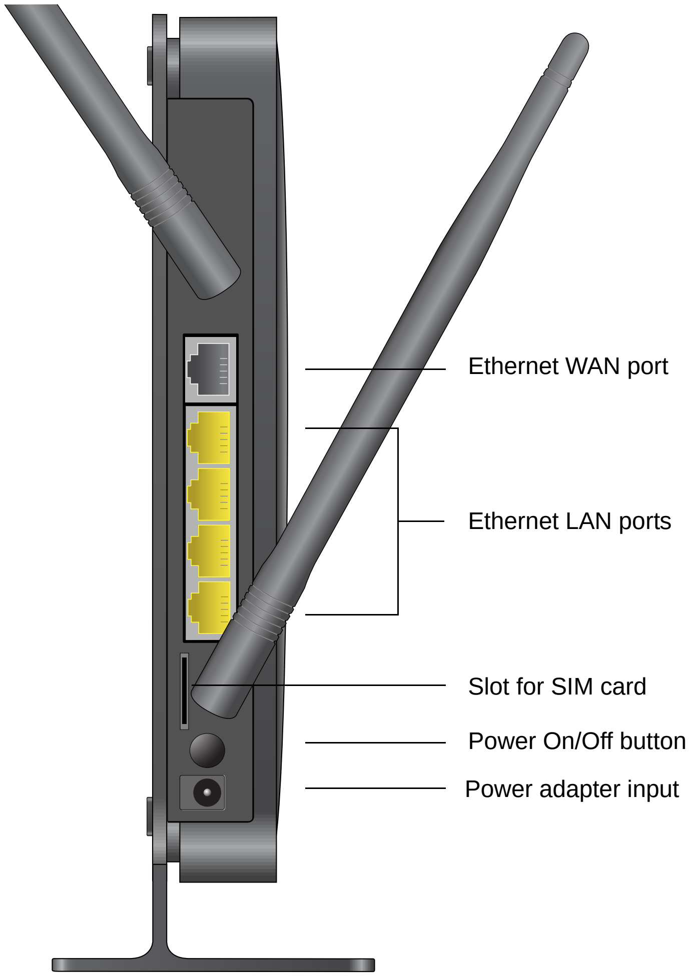
LED	Activity	Description
WPS	Press the WPS button to open a 2-minute window for the router to connect with other WPS-enabled devices. For more information about this function, see *Wi-Fi Protected Setup (WPS) Method* on page 17.	
Wireless On/Off	This button can be used to control the WiFi radio or both the WiFi radio and mobile broadband radio. Use the router interface to select the options. The default is set for WiFi radio only.	
Power	Solid green	The router is turned on and operating normally.
	Solid amber	There has been a power-on self-test failure or device failure.
	Off	Power is not supplied to the router.
Internet	Solid green	An Internet connection is established.
	Blinking green	Data is being transmitted over the Internet connection.
	Blinking green and amber	There has been a failover from WAN to mobile broadband.
	Off	No Internet connection is detected.
WiFi	Solid blue	The WiFi local port is initialized.
	Blinking blue	Data is being transmitted or received over the WiFi link.
	Off	The wireless access point is turned off.
LAN	Solid green	The local Ethernet ports have detected wired links with computers.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on the Ethernet LAN ports.
WAN	Solid green	The Ethernet WAN port has detected an active link.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on the Ethernet WAN port.
4G LTE	Solid blue	The router is in 4G LTE coverage.
	Off	No coverage is detected.

Table 1. LED descriptions (continued)

LED	Activity	Description
Signal Quality 	Solid blue	Excellent coverage is detected.
	Solid green	Good coverage is detected.
	Solid amber	Low coverage is detected.
	Off	No coverage is detected.

Router Back Panel

The back panel of the router contains port connections.

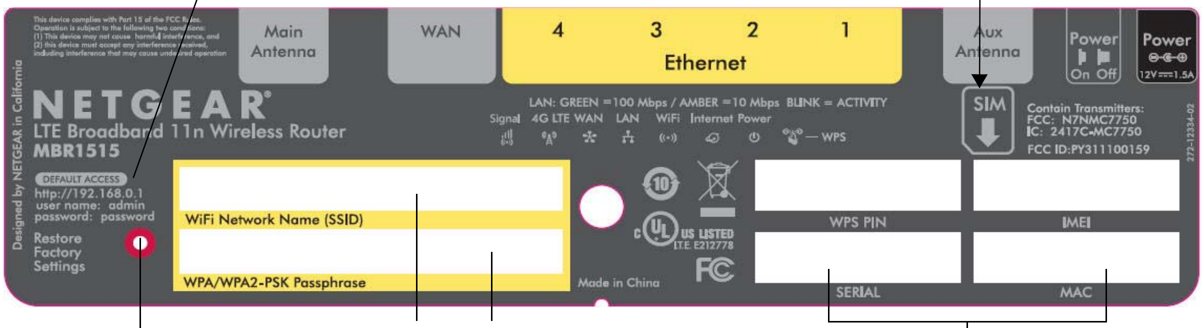


Router Label

The label on the side of the router shows the router’s MAC address, serial number, security PIN, IMEI or ESN number, and factory default login information. It also contains the SSID and passphrase that are unique to each router.

Default access address, user name, and password

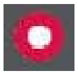
Direction of SIM card insertion


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
Designed by NETGEAR in California
Main Antenna
WAN
4
3
2
1
Ethernet
Aux Antenna
Power On Off
Power 12V⎓1.5A
NETGEAR®
LTE Broadband 11n Wireless Router
MBR1515
LAN: GREEN =100 Mbps / AMBER =10 Mbps BLINK = ACTIVITY
Signal 4G LTE WAN LAN WiFi Internet Power
WPS
SIM
Contain Transmitters:
FCC: N7NMC7750
IC: 2417C-MC7750
FCC ID:PY311100159
272-12334-02
DEFAULT ACCESS
http://192.168.0.1
user name: admin
password: password
Restore Factory Settings
WiFi Network Name (SSID)
WPA/WPA2-PSK Passphrase
10
c UL US LISTED I.T.E. E212778
FC
Made in China
WPS PIN
IMEI
SERIAL
MAC

Restore Factory Settings: Press for 6 seconds

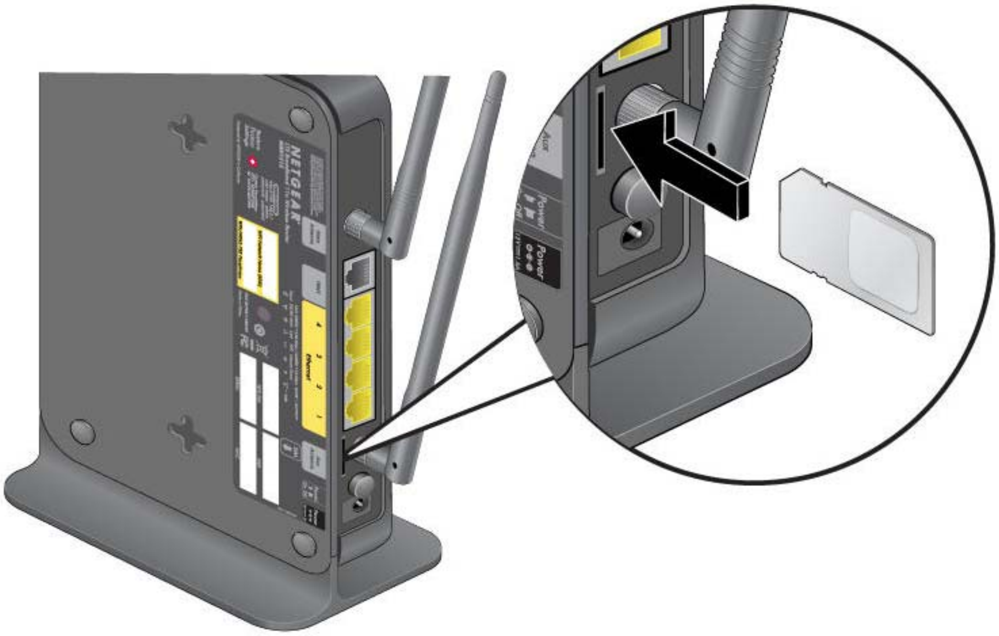
Router label with unique SSID and passphrase

Router information
- WPS security PIN
- IMEI or ESN number
- Serial number
- MAC address

Restore Factory Settings 	Locate the small hole outlined in red on the side of the router. Insert a paperclip into the hole and press for 6 seconds. Pressing the **Restore Factory Settings** button causes the Power LED to blink briefly. After the button is held down for more than 6 seconds, the Power LED flashes amber and turns green as the router resets to the factory defaults.

Insert the SIM Card

If your router did not come with a SIM already installed, then gently insert an active Verizon SIM card into the SIM card slot on the back of the router. You should hear a “click” sound when the SIM card has been inserted properly. The SIM card can be acquired from your authorized Verizon wireless retailer.



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.

Use the Signal Quality LED on the front panel to position the router for best signal strength. Also for best results, place your router:

- On an upper floor of a multifloor home or office.
- Close to a window but avoiding direct sunlight. A window location gives the best conditions for receiving a strong 4G signal strength.
- 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, such as ceiling fans, home security systems, microwaves, computers, or the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

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 5 channels (for example, use Channels 1 and 6, or 6 and 11).

2. Getting Started with NETGEAR genie

Connecting to the router

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

This chapter contains the following sections:

- *Router Setup*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use the NETGEAR genie*
- *Router Dashboard (BASIC Home Screen)*
- *Add Wireless Devices or Computers to Your Network*

Router Setup

The router comes with a default configuration. If you want to change from the default configuration, you can use the NETGEAR genie menus and screens to set up your router manually. However, before you start the setup process, you have to have your ISP information available and make sure the laptops, computers, and other devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

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

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the router.

Types of Logins and Access

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

- **Router login** logs you in to the router interface from NETGEAR genie. See *Use the NETGEAR genie* on page 15 for details about this login.
- **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.

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

1. Turn the router on by pressing the **On/Off** button, if not done yet.
2. Make sure that your device is connected with an Ethernet cable (wired) or wirelessly (with the preset security settings listed on the bottom label) to your router.
3. Launch your Internet browser.
    - If this session is the first time you are setting up the Internet connection for your router, the browser automatically goes to http://192.168.0.1, and the NETGEAR genie screen displays.

- If you already used the NETGEAR genie, type **http://192.168.0.1** in the address field for your browser to display the NETGEAR genie screen. See *Use the NETGEAR genie* on page 15.

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 is ready to use. Its Power LED should light.
- Close and reopen the browser to make sure that the browser does not cache the previous page.
- Browse to **http://192.168.0.1**.
- If the computer is set to a static or fixed IP address (this type of setting is uncommon), change the setting to obtain an IP address automatically from the router.

If the router does not connect to the Internet:

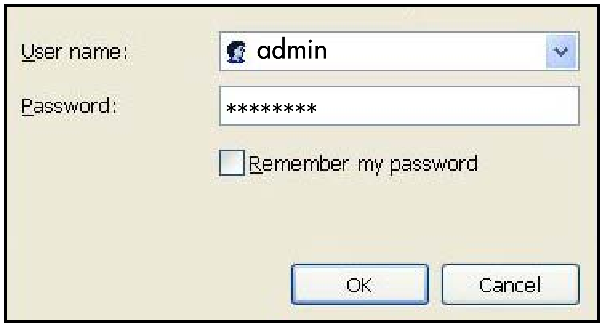
1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 8, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR technical support.

Use the NETGEAR genie

You can use NETGEAR genie if you want to view or change settings for the router.

1. Launch your browser from a computer or wireless device that is connected to the router.
2. Type **http://192.168.0.1**.

   The login screen displays:



User name: admin

Password: ********

□ Remember my password

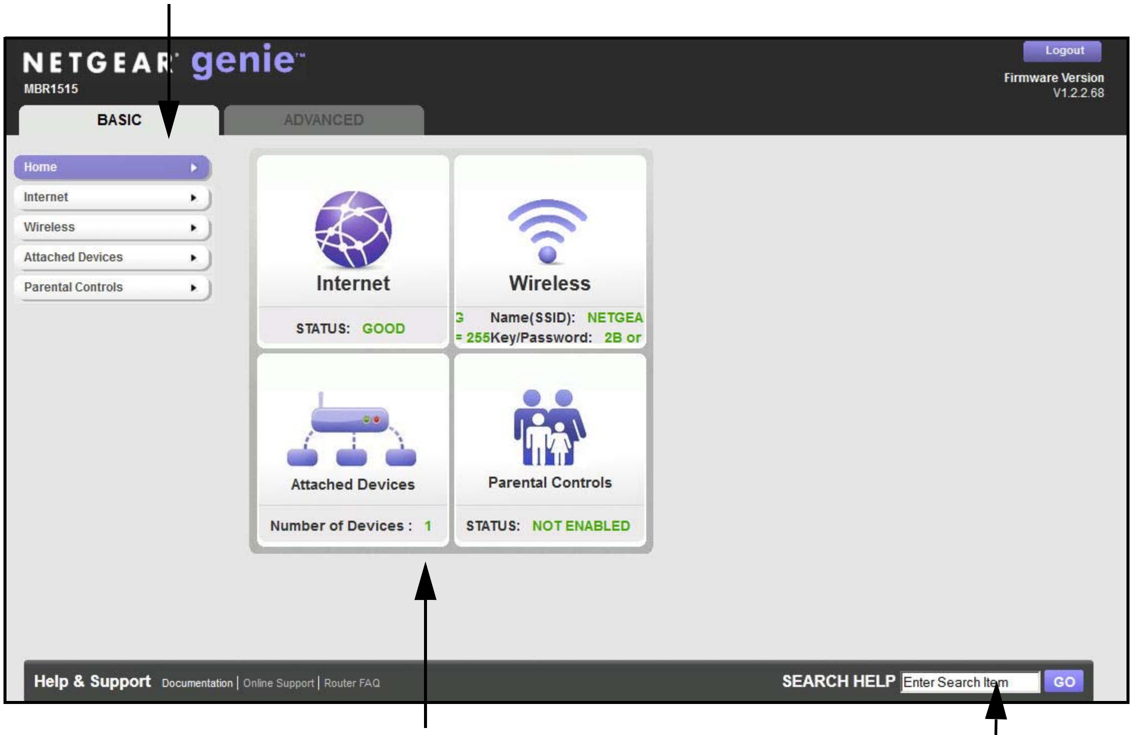
3. Enter **admin** for the router user name and **password** for the router password, both in lowercase letters.

Note: *The router user name and password are different from the user name and password for logging in to your Internet connection. See Types of Logins and Access on page 14 for more information.*

Router 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 four sections of the dashboard to view more detailed information. The left column has the menus, and at the top is an ADVANCED tab that is used to access more menus and screens.

Menus (Click the ADVANCED tab to view more)



STATUS: GOOD

Name(SSID): NETGEA

Key/Password: 2B or

Number of Devices : 1

STATUS: NOT ENABLED

Dashboard (Click to view details) **Help**

- **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.
- **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 7, Advanced Settings*. Using this tab requires a solid understanding of networking concepts.

- **Help & Support**. Go to the NETGEAR support site for information, help, and product documentation. These links work once you have an Internet connection.

Add Wireless Devices or Computers to Your Network

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

Manual Method

➢ **To connect manually:**

1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your router. This software scans for all wireless networks in your area.
2. Look for your network and select it. If you did not change the name of your network during the setup process, look for the default WiFi network name (SSID) and select it. The default SSID is on the product label on the bottom of the router.
3. Enter the router password and click **Connect**. The default router passphrase is on the product label on the bottom of the router.
4. Repeat steps 1–3 to add other wireless devices.

Wi-Fi Protected Setup (WPS) Method

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

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

If your wireless device supports WPS (Push 'N' Connect), follow these steps:

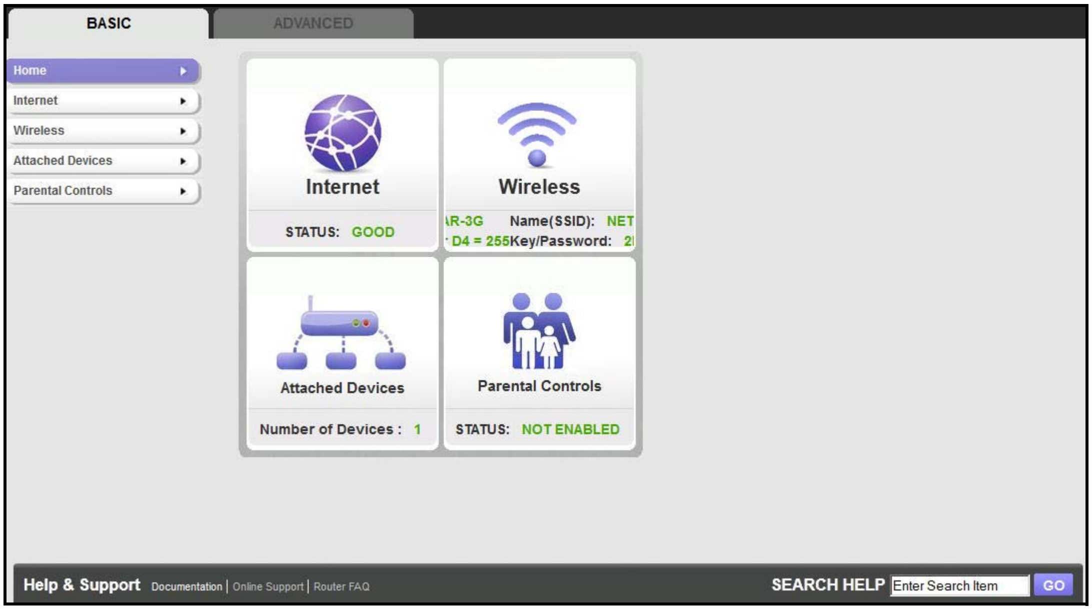
1. Press the **WPS** button on the router front panel.
2. Within 2 minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device. The device is now connected to your router.
3. Repeat steps 1–2 to add other WPS wireless devices.

NETGEAR genie BASIC Settings

3

Your Internet connection and network

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



STATUS: GOOD

\R-3G Name(SSID): NET

· D4 = 255Key/Password: 2

Number of Devices : 1

STATUS: NOT ENABLED

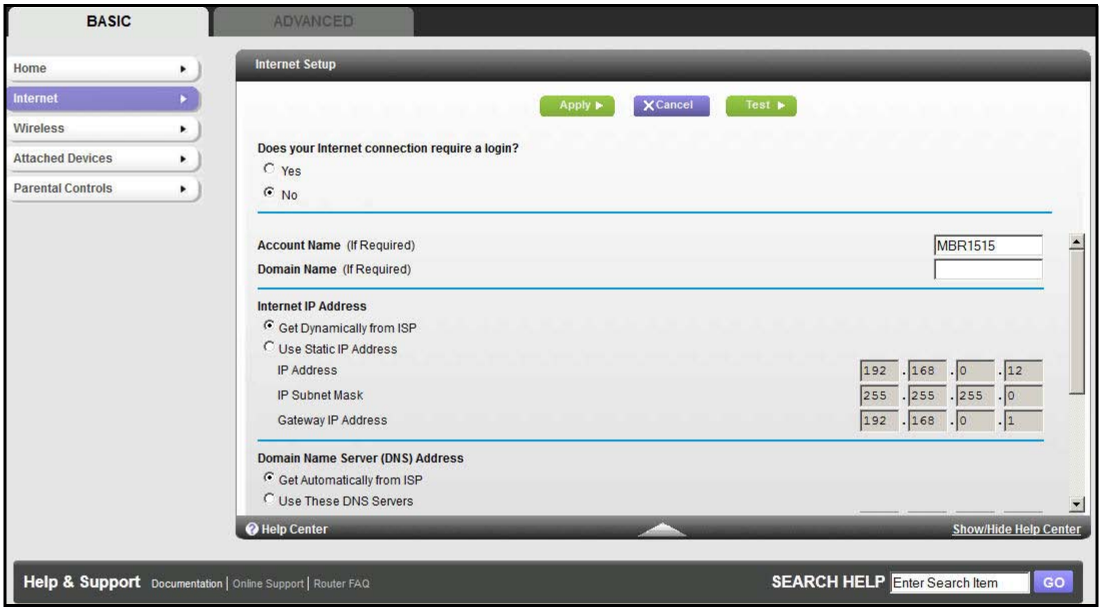
This chapter contains the following sections:

- *Internet Setup*
- *Wireless Settings*
- *Attached Devices*
- *Parental Controls*

Internet Setup

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

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



Internet Setup

Does your Internet connection require a login?

○ Yes

● No

Account Name (If Required) MBR1515

Domain Name (If Required)

Internet IP Address

● Get Dynamically from ISP

○ Use Static IP Address

IP Address 192 . 168 . 0 . 12

IP Subnet Mask 255 . 255 . 255 . 0

Gateway IP Address 192 . 168 . 0 . 1

Domain Name Server (DNS) Address

● Get Automatically from ISP

○ Use These DNS Servers

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

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

2. Enter the settings for the IP address and DNS server. The default settings usually work fine. If you have problems with your connection, check the ISP settings.
3. Click **Apply** to save your settings.
4. Click **Test** to test your Internet connection. If the NETGEAR website does not display within 1 minute, see *Chapter 8, Troubleshooting*.

Internet Setup Screen Fields

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

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

These fields display when no login is required:

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

These fields display when your ISP requires a login:

- **Login**. The login name provided by your ISP. This name is often an email address.
- **Password**. The password that you use to log in to your ISP.
- **Idle Timeout (In minutes)**. If you want to change the login timeout, enter a new value in minutes. This value determines how long the router keeps the Internet connection active after no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP 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 does not automatically transmit DNS addresses to the router during login, select this option, and enter the IP address of your ISP primary DNS server. If a secondary DNS server address is available, enter it also.

Router MAC Address. The Ethernet MAC address used by the router on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They then accept traffic only from the MAC address of that computer. This feature allows your router to use your computer's MAC address (this process is 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 is allowed by the ISP.
- **Use This MAC Address**. Enter the MAC address that you want to use.

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 WiFi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the bottom of the unit.

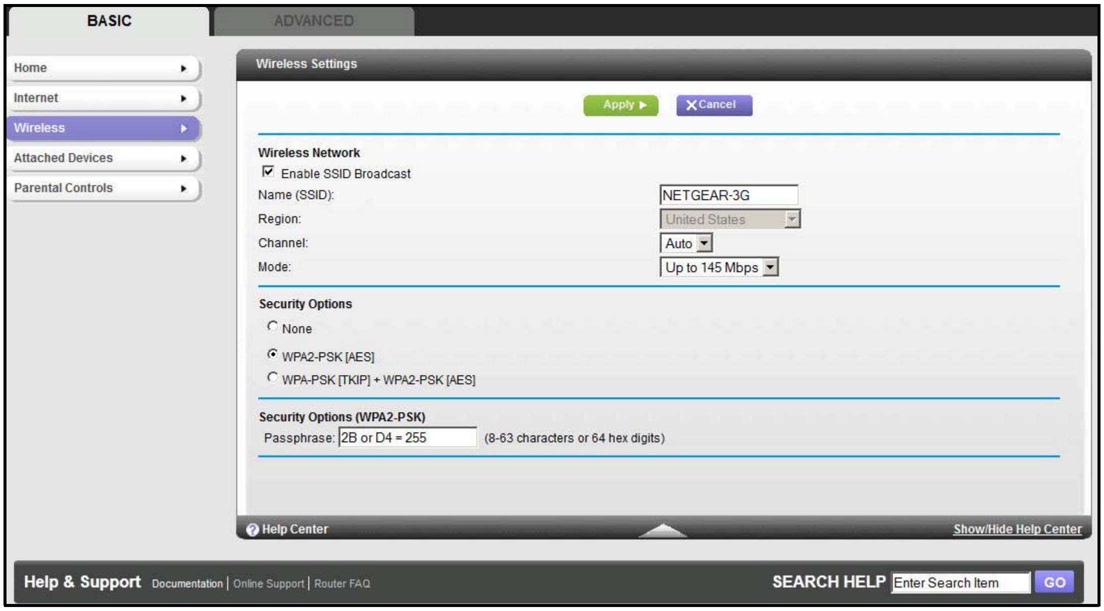
Note: The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

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

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

➢ To view or change basic wireless settings:

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



Wireless Network

☑ Enable SSID Broadcast

Name (SSID): NETGEAR-3G

Region: United States

Channel: Auto

Mode: Up to 145 Mbps

Security Options

○ None

● WPA2-PSK [AES]

○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Options (WPA2-PSK)

Passphrase: 2B or D4 = 255 (8-63 characters or 64 hex digits)

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

2. Make any changes that are needed, and click **Apply** to save your settings.
3. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:

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

Wireless Settings Screen Fields

Wireless Network

The b/g/n and a/n notation references the 802.11 standards of conformance. For example, the 2.4 b/g/n conforms to 802.11b, 802.11g, and 802.11n at the 2.4 GHz radio frequency.

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 the **Enable SSID Broadcast** check box, and click **Apply**.

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 Selection. 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. This setting is the wireless channel used by the gateway. Enter a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). When interference happens, experiment with different channels to see which is the best.

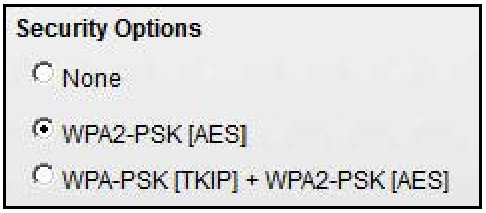
Mode. Up to 145 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. The 300 Mbps setting allows 802.11n devices to connect at this speed.

Security Options

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. ***NETGEAR recommends that you do not change the security option or passphrase,*** but if you want to change these settings, the following section explains how. ***Do not disable security***.

Change WPA Security Option and Passphrase

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



Security Options

○ None

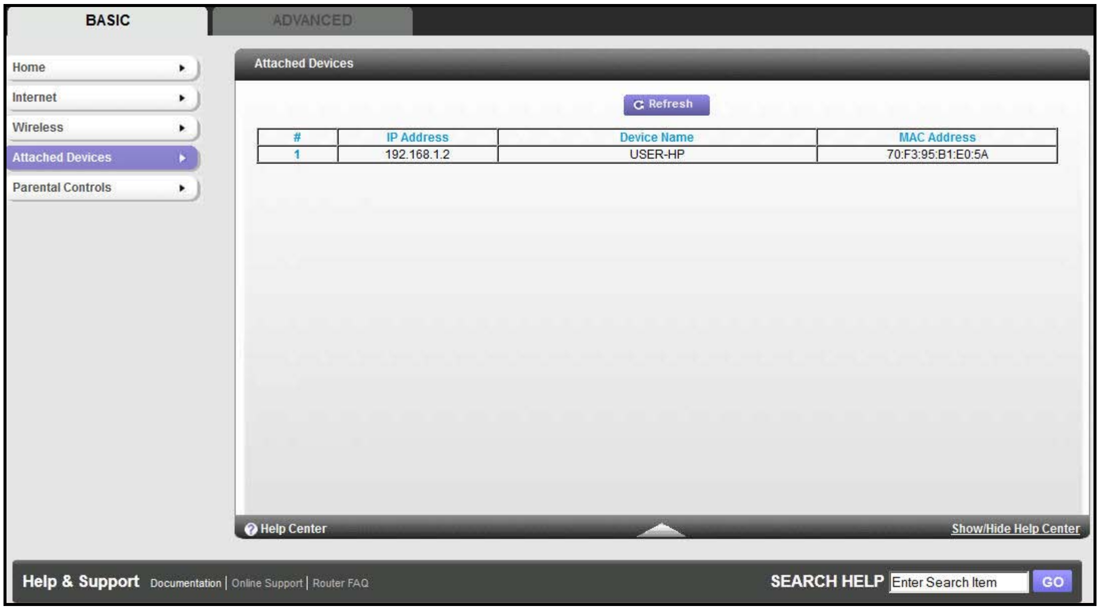
● WPA2-PSK [AES]

○ WPA-PSK [TKIP] + WPA2-PSK [AES]

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

Attached Devices

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



#	IP Address	Device Name	MAC Address
1	192.168.1.2	USER-HP	70:F3:95:B1:E0:5A

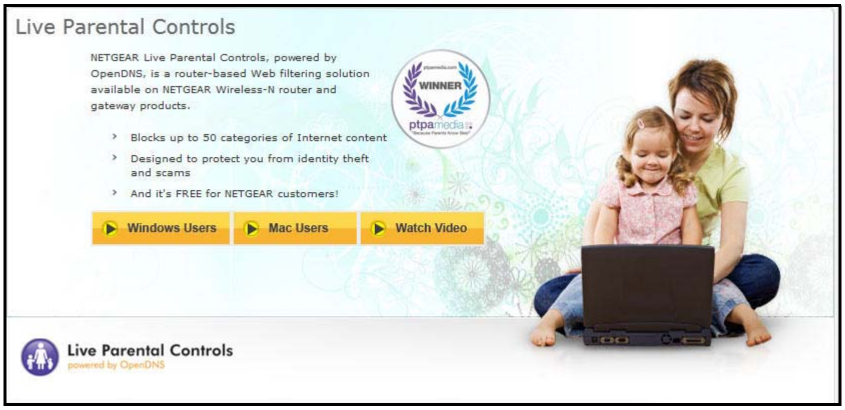
Wired devices are connected to the router with Ethernet cables. Wireless devices have joined the wireless network.

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

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

Parental Controls

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



Live Parental Controls

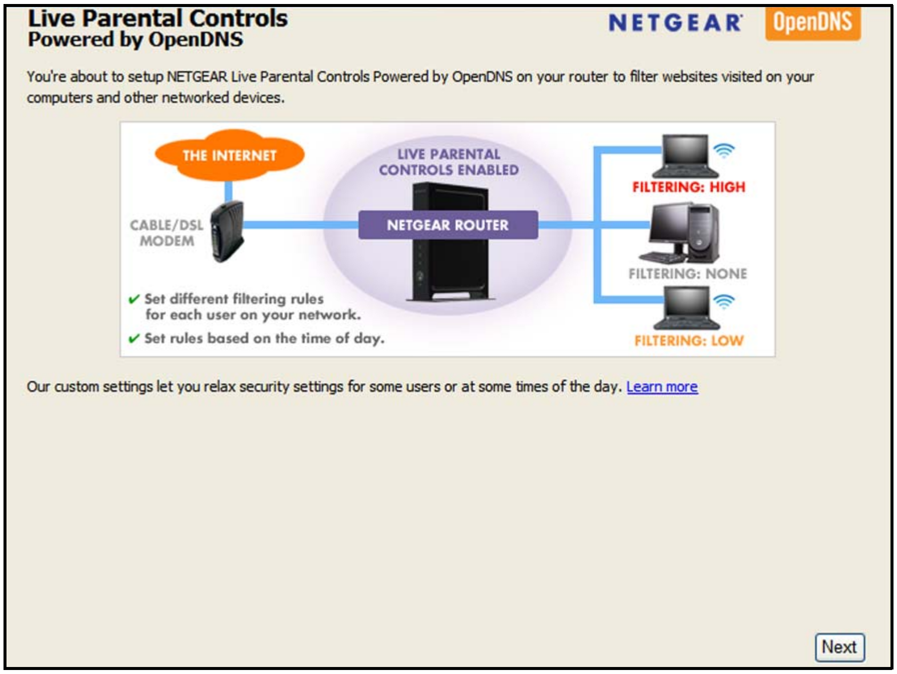
NETGEAR Live Parental Controls, powered by OpenDNS, is a router-based Web filtering solution available on NETGEAR Wireless-N router and gateway products.

- Blocks up to 50 categories of Internet content
- Designed to protect you from identity theft and scams
- And it's FREE for NETGEAR customers!

➤ **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.



Live Parental Controls
Powered by OpenDNS

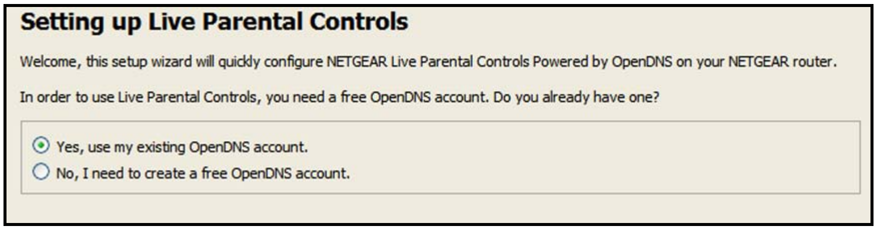
You're about to setup NETGEAR Live Parental Controls Powered by OpenDNS on your router to filter websites visited on your computers and other networked devices.

✔ Set different filtering rules for each user on your network.
✔ Set rules based on the time of day.

Our custom settings let you relax security settings for some users or at some times of the day. Learn more

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

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



Setting up Live Parental Controls

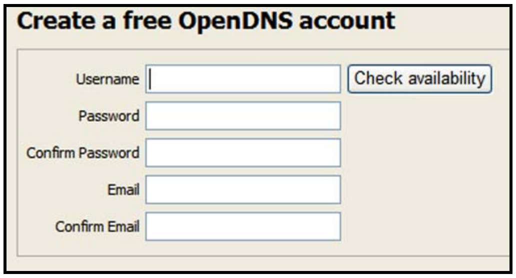
Welcome, this setup wizard will quickly configure NETGEAR Live Parental Controls Powered by OpenDNS on your NETGEAR router.

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

● Yes, use my existing OpenDNS account.
○ No, I need to create a free OpenDNS account.

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

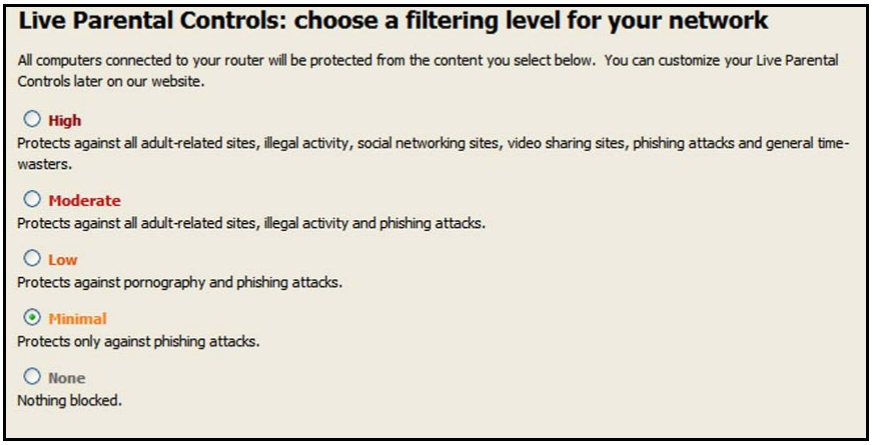


Create a free OpenDNS account

Username	
Password	
Confirm Password	
Email	
Confirm Email	

   - Fill in the fields and click **Next**.

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



Live Parental Controls: choose a filtering level for your network

All computers connected to your router will be protected from the content you select below. You can customize your Live Parental Controls later on our website.

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

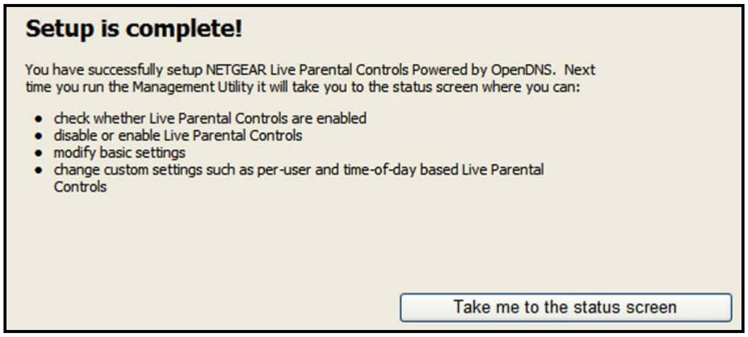
○ **Moderate**
Protects against all adult-related sites, illegal activity and phishing attacks.

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

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

○ **None**
Nothing blocked.

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



Setup is complete!

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

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

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

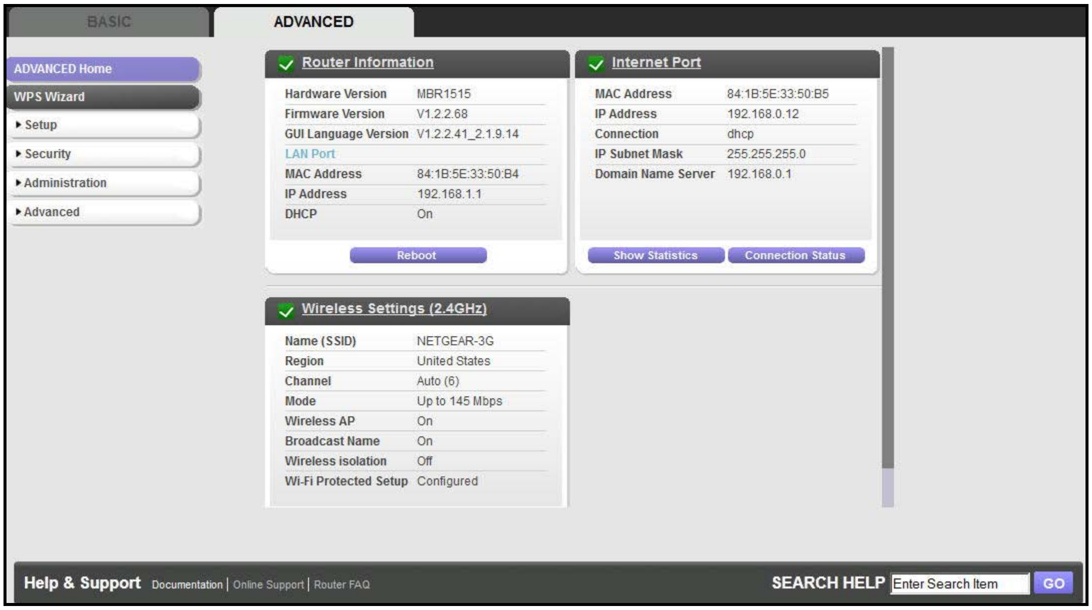
Parental controls are now set up for the router. The dashboard shows Parental Controls as Enabled.

NETGEAR genie ADVANCED Home

Specifying custom settings

4

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



Router Information

Hardware Version	MBR1515
Firmware Version	V1.2.2.68
GUI Language Version	V1.2.2.41_2.1.9.14
LAN Port	
MAC Address	84:1B:5E:33:50:B4
IP Address	192.168.1.1
DHCP	On

Internet Port

MAC Address	84:1B:5E:33:50:B5
IP Address	192.168.0.12
Connection	dhcp
IP Subnet Mask	255.255.255.0
Domain Name Server	192.168.0.1

Wireless Settings (2.4GHz)

Name (SSID)	NETGEAR-3G
Region	United States
Channel	Auto (6)
Mode	Up to 145 Mbps
Wireless AP	On
Broadcast Name	On
Wireless isolation	Off
Wi-Fi Protected Setup	Configured

This chapter contains the following sections:

- *WPS Wizard*
- *Setup Menu*
- *Broadband Settings*
- *Mobile Broadband Settings*
- *WAN Setup*
- *LAN Setup*
- *Quality of Service Setup*

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

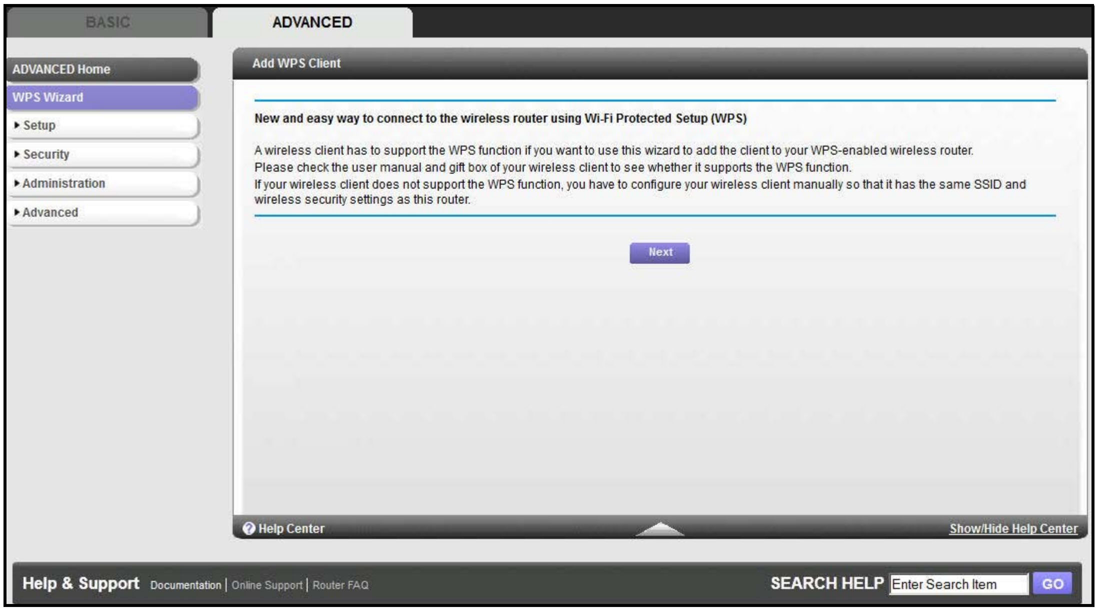
- **Security**. See *Chapter 5, Security*.
- **Administration**. See *Chapter 6, Administration*.
- **Advanced Setup**. See *Chapter 7, Advanced Settings*.

WPS Wizard

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

➢ **To use the WPS Wizard:**

1. Select **ADVANCED > WPS Wizard**.
2. Click **Next**. The following screen lets you select the method for adding the WPS client (a wireless device or computer).

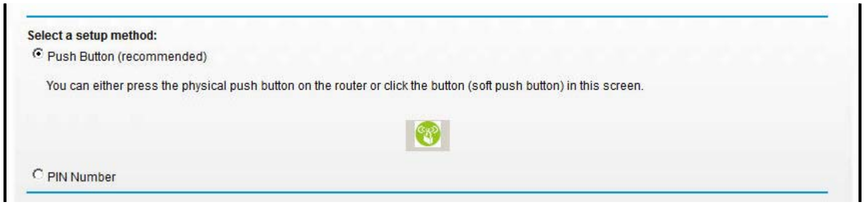


New and easy way to connect to the wireless router using Wi-Fi Protected Setup (WPS)

A wireless client has to support the WPS function if you want to use this wizard to add the client to your WPS-enabled wireless router.
Please check the user manual and gift box of your wireless client to see whether it supports the WPS function.
If your wireless client does not support the WPS function, you have to configure your wireless client manually so that it has the same SSID and wireless security settings as this router.

You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.
   - To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button on the side of the router. Within 2 minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.

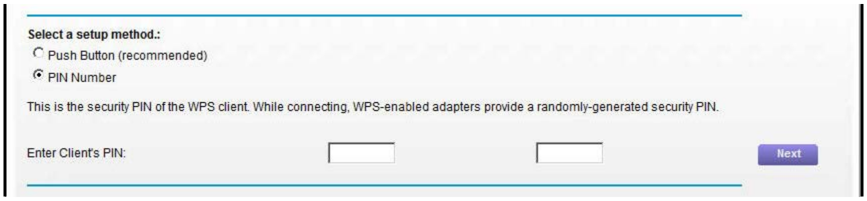


Select a setup method:
● Push Button (recommended)

You can either press the physical push button on the router or click the button (soft push button) in this screen.

○ PIN Number

- To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click **Next**.



Select a setup method.:

○ Push Button (recommended)

● PIN Number

This is the security PIN of the WPS client. While connecting, WPS-enabled adapters provide a randomly-generated security PIN.

Enter Client's PIN:

Within 2 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.

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

Setup Menu

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

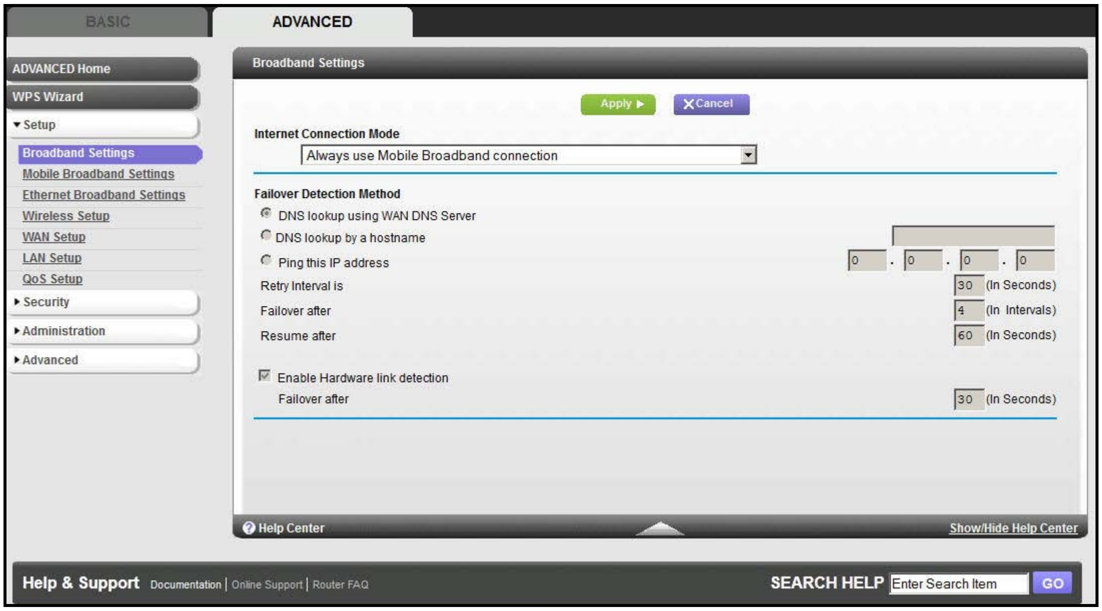
- **Broadband Settings**. Configure the Internet connection mode of your router. See *Broadband Settings* on page 30.
- **Mobile Broadband Settings**. Configure the access to your mobile broadband account. See *Mobile Broadband Settings* on page 30.
- **Ethernet Broadband Settings**. This menu item is a shortcut to the same Internet Setup screen that you can access from the dashboard on the BASIC Home screen. See *Internet Setup* on page 19.
- **Wireless Setup**. This menu item is a shortcut to the same Wireless Settings screen that you can access from the dashboard on the BASIC Home screen. See *Wireless Settings* on page 21.
- **WAN Setup**. Internet (WAN) setup. See *WAN Setup* on page 32.
- **LAN Setup**. Local area network (LAN) setup. See *LAN Setup* on page 35.
- **QoS Setup**.Quality of Service (QoS) setup. See *Quality of Service Setup* on page 38.

Broadband Settings

The Broadband Settings screen lets you select the Internet connection mode of your router.

➤ **To select your Internet connection mode:**

1. Select **ADVANCED > Setup > Broadband Settings** to view the following screen:



Internet Connection Mode: Always use Mobile Broadband connection

Failover Detection Method

● DNS lookup using WAN DNS Server

○ DNS lookup by a hostname

○ Ping this IP address 0 . 0 . 0 . 0

Retry Interval is 30 (In Seconds)

Failover after 4 (In Intervals)

Resume after 60 (In Seconds)

☑ Enable Hardware link detection

Failover after 30 (In Seconds)

Your Internet connection choices include the following:

- Use Ethernet connection first and if fail use mobile broadband connection
- Always use Mobile Broadband connection
- Always use Ethernet connection

2. Click **Apply** to save your selection.

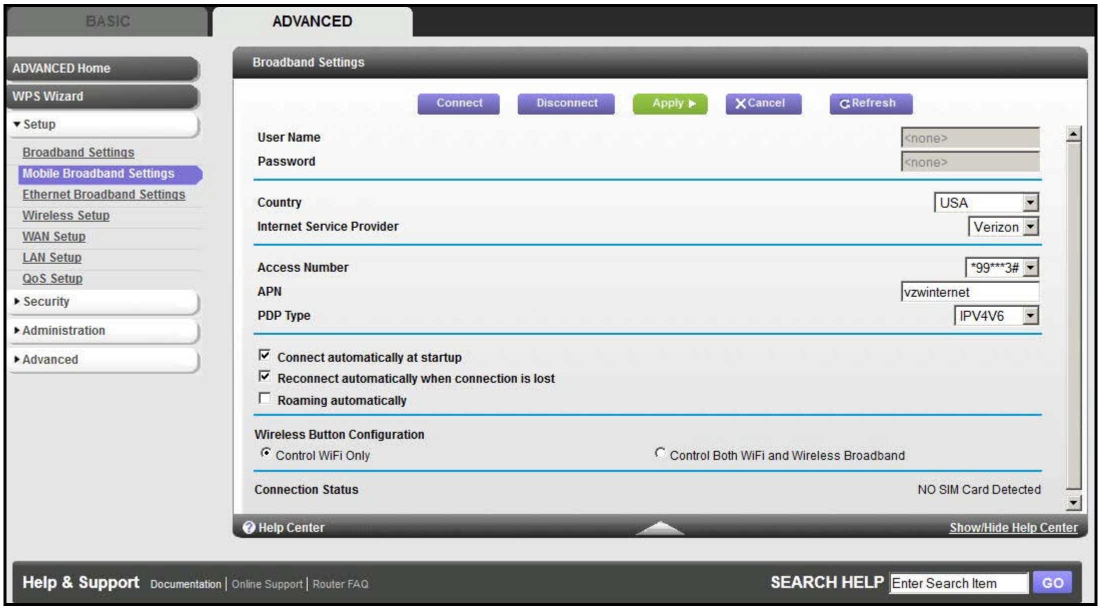
Mobile Broadband Settings

The Mobile Broadband Settings screen lets you configure the access to your mobile broadband account.

Note: Connecting to the mobile broadband network requires an active broadband service account.

➢ To configure your mobile broadband account access:

1. Select **ADVANCED > Setup > Mobile Broadband Settings** to view the following screen:



User Name <none>
Password <none>

Country USA
Internet Service Provider Verizon

Access Number *99***3#
APN vzwinternet
PDP Type IPV4V6

☑ Connect automatically at startup
☑ Reconnect automatically when connection is lost
☐ Roaming automatically

Wireless Button Configuration
● Control WiFi Only ○ Control Both WiFi and Wireless Broadband

Connection Status NO SIM Card Detected

The following settings are provided:

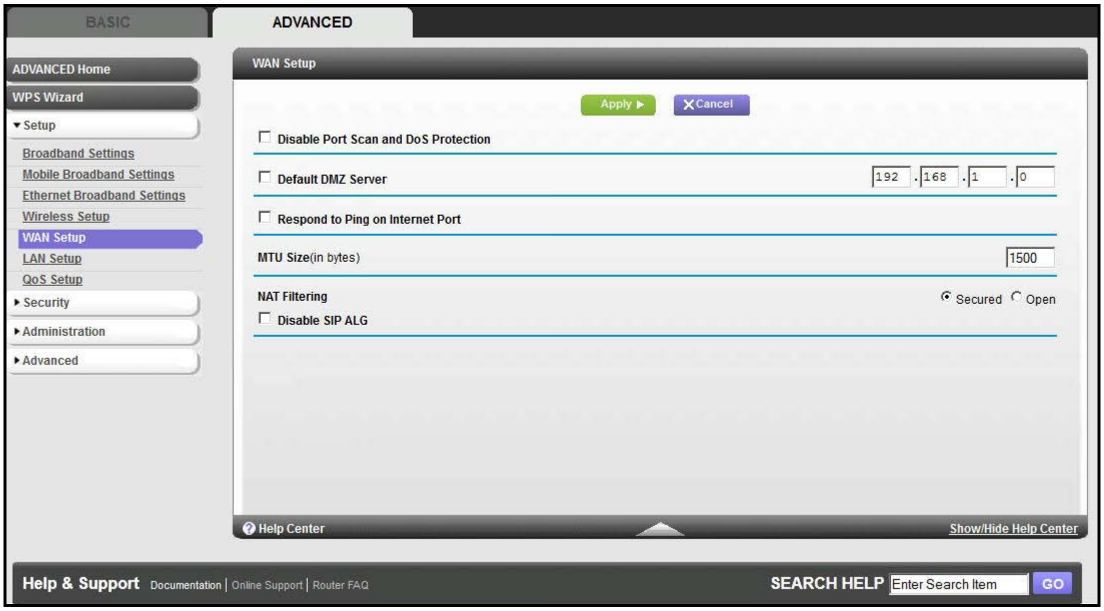
- **User Name**. The account login user name.
- **Password**. The account password for authentication.
- **Country**. The country where mobile broadband service is provided.
- **Internet Service Provider**. The Internet service provider of the 4G network.
- **PIN code**. The PIN code of the SIM card if the PIN has been enabled.
- **Access Number**. The phone number of the remote site.
- **APN**. The access point name.
- **PDP Type**. The type of packet data protocol.
- **Connect automatically at startup**. When this check box is selected, the modem automatically connects to the network when powered up. This check box should be selected after login information is provided.
- **Reconnect automatically when connection is lost**. When this check box is selected, the modem attempts to reconnect to the network when the connection is lost. Under normal situations, this setting should be selected.
- **Roaming automatically**. When this check box is checked, the unit might roam to any available operator in range and might incur roaming charges.
- **Wireless Button Configuration**. Choose whether you want the WPS button to control WiFi only or both WiFi and wireless broadband.
- **Connection Status**. The status of the current WAN port.

2. Click **Apply** to save your settings.
3. Click **Connect** when you want to connect manually to the network.

4. Click **Disconnect** when you want to disconnect manually from the current network.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the router to respond to a ping on the WAN (Internet) port. Select **ADVANCED > Setup > WAN Setup** to view the following screen:



□ Disable Port Scan and DoS Protection

□ Default DMZ Server 192 . 168 . 1 . 0

□ Respond to Ping on Internet Port

MTU Size(in bytes) 1500

NAT Filtering ● Secured ○ Open

□ Disable SIP ALG

- **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 setting 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 *Default DMZ Server* on page 33 for more details.
- **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 only as a diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.
- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. This reduction is rarely required, and should not be done unless you are sure that it is necessary for your ISP connection. See *Change the MTU Size* on page 33.
- **NAT Filtering**. Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall but allows almost all Internet applications to function.

- **Disable SIP ALG**. Some VoIP applications do not work well with the SIP ALG. Selecting this check box to turn off the SIP ALG helps your VoIP devices create and accept calls through the router.

Default DMZ Server

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

WARNING:

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

Incoming traffic from the Internet gets discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. On the WAN Setup screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. Click **Apply**.

Change the MTU Size

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If any device in the data path has a lower MTU setting than the other devices, the data packets have to be split or "fragmented" to accommodate the device with the smallest MTU.

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value might fix one problem but cause another. Leave 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 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 causes Internet communication problems such as the inability to access certain websites, frames within websites, secure login pages, and 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 and the default value. This value is the typical setting for non-PPPoE, non-VPN connections and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➢ To change the MTU size:

1. Select **ADVANCED > Setup > WAN Setup**.
2. In the MTU Size field, enter a new size from 64 through 1500.
3. Click **Apply** to save the settings.

LAN Setup

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

The 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:

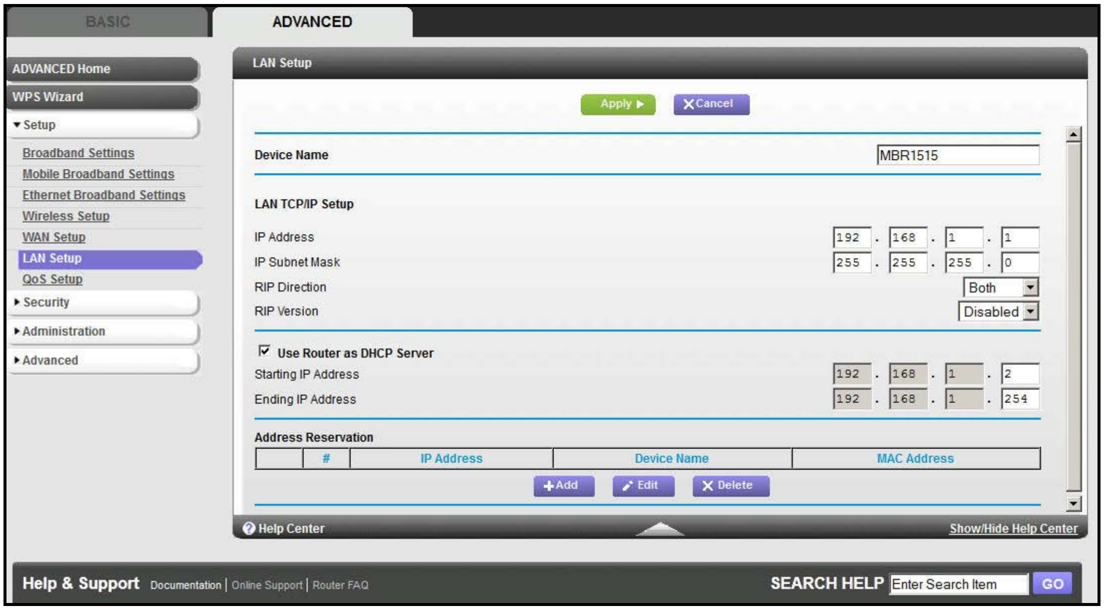
- LAN IP address. **192.168.0.1**
- Subnet mask. **255.255.255.0**

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

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

➢ To change the LAN settings:

1. Select **ADVANCED > Setup > LAN Setup** to display the following screen:



LAN Setup

Device Name: MBR1515

LAN TCP/IP Setup

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: Both

RIP Version: Disabled

☑ Use Router as DHCP Server

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 254

Address Reservation

	#	IP Address	Device Name	MAC Address

2. Enter the settings that you want to customize. These settings are described in *LAN Setup Screen Settings* on page 36.
3. Click **Apply** to save your changes.

LAN Setup Screen Settings

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 a DHCP Server

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

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

Use the Router as a DHCP Server

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

You can specify the pool of IP addresses that are assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should 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 you have defined
- Subnet mask
- Gateway IP address (the router's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Internet Setup screen; otherwise, the router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Internet Setup screen)

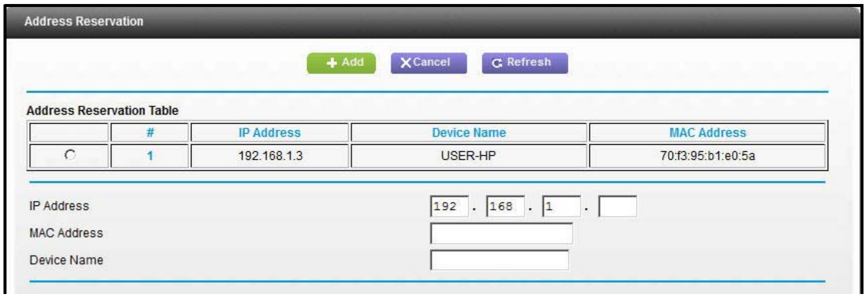
To use another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, you have to set your computers' IP addresses manually or they are not able to access the router.

Address Reservation

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

➢ **To reserve an IP address:**

1. In the Address Reservation section of the screen, click the **Add** button to display the following screen:



Address Reservation

Address Reservation Table

	#	IP Address	Device Name	MAC Address
○	1	192.168.1.3	USER-HP	70:f3:95:b1:e0:5a

IP Address	192 . 168 . 1 .
MAC Address	
Device Name	

2. 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.)
3. Type the MAC address of the computer or server.

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

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

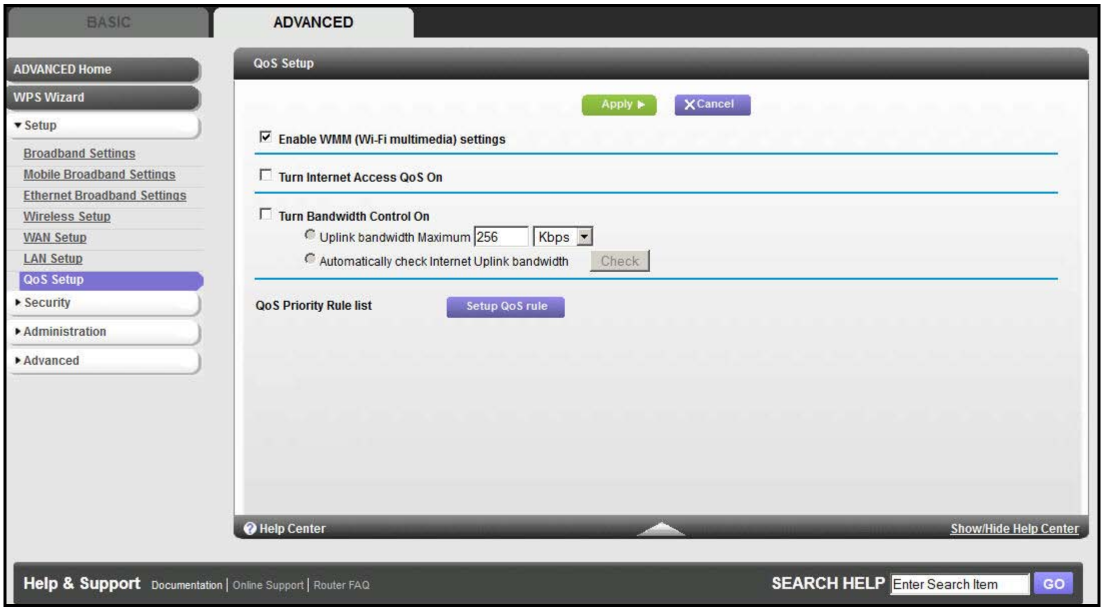
The reserved address is not assigned until the next time the computer contacts the router’s DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

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

Quality of Service Setup

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

Select **ADVANCED > Setup > QoS Setup** to display the following screen:



☑ Enable WMM (Wi-Fi multimedia) settings

□ Turn Internet Access QoS On

□ Turn Bandwidth Control On

○ Uplink bandwidth Maximum 256 Kbps

○ Automatically check Internet Uplink bandwidth

QoS Priority Rule list

Enable WMM QoS for Wireless Multimedia Applications

WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities depending on the type of data. Time-dependent information, such as video and audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients have to support WMM also.

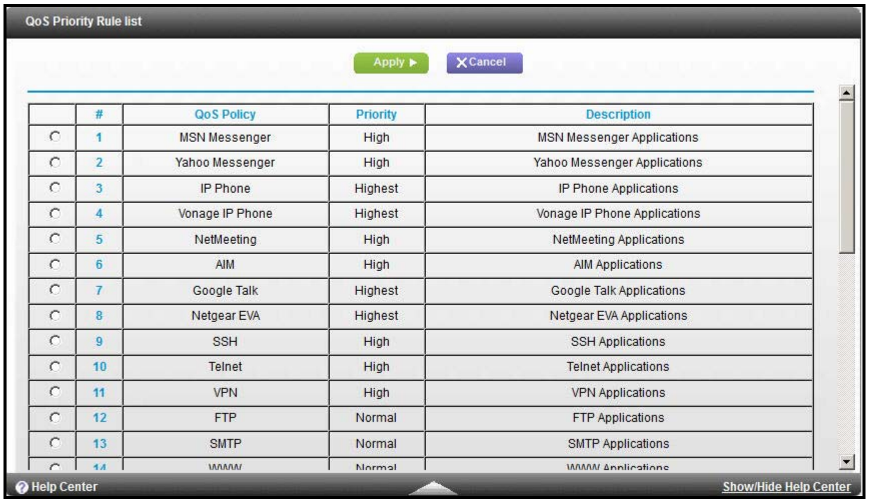
WMM QoS is enabled by default. You can disable it in the QoS Setup screen by clearing the **Enable WMM (Wi-Fi multimedia) settings** check box and clicking **Apply**.

Turn Internet Access QoS On

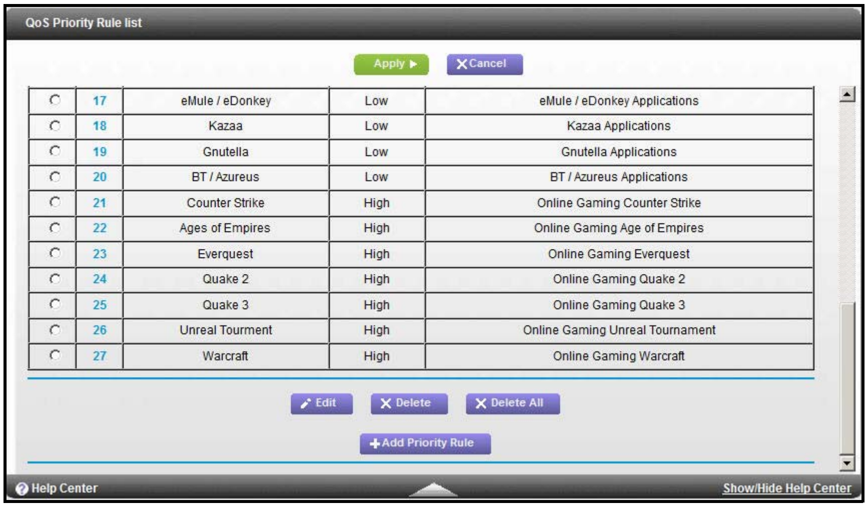
Enable this feature for the QoS function to prioritize Internet traffic.

Manage the QoS Priority Rules

Select **ADVANCED > Setup > QoS Setup** and click the **Setup QoS rule button** to display the following screen:



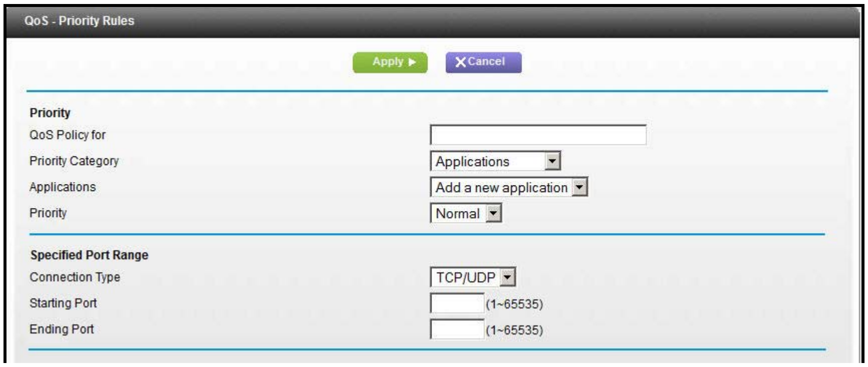
	#	QoS Policy	Priority	Description
○	1	MSN Messenger	High	MSN Messenger Applications
○	2	Yahoo Messenger	High	Yahoo Messenger Applications
○	3	IP Phone	Highest	IP Phone Applications
○	4	Vonage IP Phone	Highest	Vonage IP Phone Applications
○	5	NetMeeting	High	NetMeeting Applications
○	6	AIM	High	AIM Applications
○	7	Google Talk	Highest	Google Talk Applications
○	8	Netgear EVA	Highest	Netgear EVA Applications
○	9	SSH	High	SSH Applications
○	10	Telnet	High	Telnet Applications
○	11	VPN	High	VPN Applications
○	12	FTP	Normal	FTP Applications
○	13	SMTP	Normal	SMTP Applications
○	14	WWW	Normal	WWW Applications



○	17	eMule / eDonkey	Low	eMule / eDonkey Applications
○	18	Kazaa	Low	Kazaa Applications
○	19	Gnutella	Low	Gnutella Applications
○	20	BT / Azureus	Low	BT / Azureus Applications
○	21	Counter Strike	High	Online Gaming Counter Strike
○	22	Ages of Empires	High	Online Gaming Age of Empires
○	23	Everquest	High	Online Gaming Everquest
○	24	Quake 2	High	Online Gaming Quake 2
○	25	Quake 3	High	Online Gaming Quake 3
○	26	Unreal Tourment	High	Online Gaming Unreal Tournament
○	27	Warcraft	High	Online Gaming Warcraft

For applications such as online gaming, an Ethernet LAN port, or a specified MAC address that already appears in the list, modify the priority level by selecting it and then clicking **Edit**. Click **Delete** to erase the priority rule.

You can also define the priority policy for each online game, application, LAN port, or the computer’s MAC address by clicking **Add Priority Rule**.



Priority

QoS Policy for

Priority Category: Applications

Applications: Add a new application

Priority: Normal

Specified Port Range

Connection Type: TCP/UDP

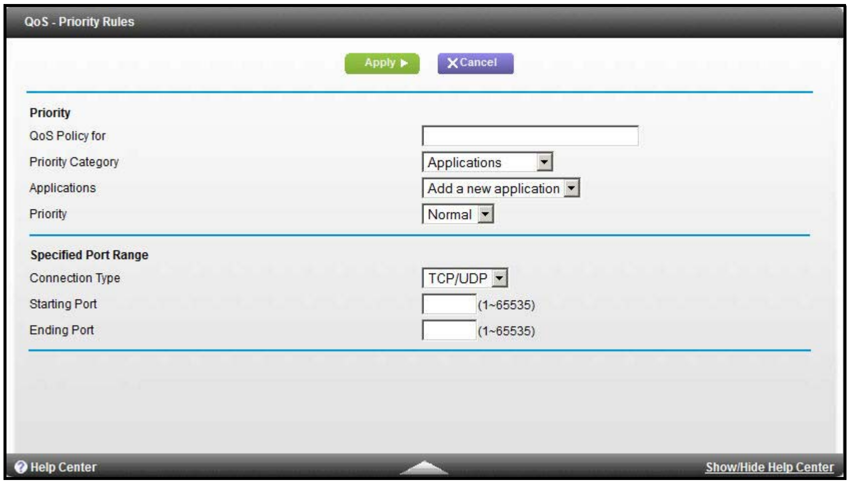
Starting Port: (1~65535)

Ending Port: (1~65535)

For Applications or Online Gaming

➤ **To set up the priority for an application or online gaming:**

1. From the Priority Category list, select **Applications** or **Online Gaming**.



Priority

QoS Policy for

Priority Category: Applications

Applications: Add a new application

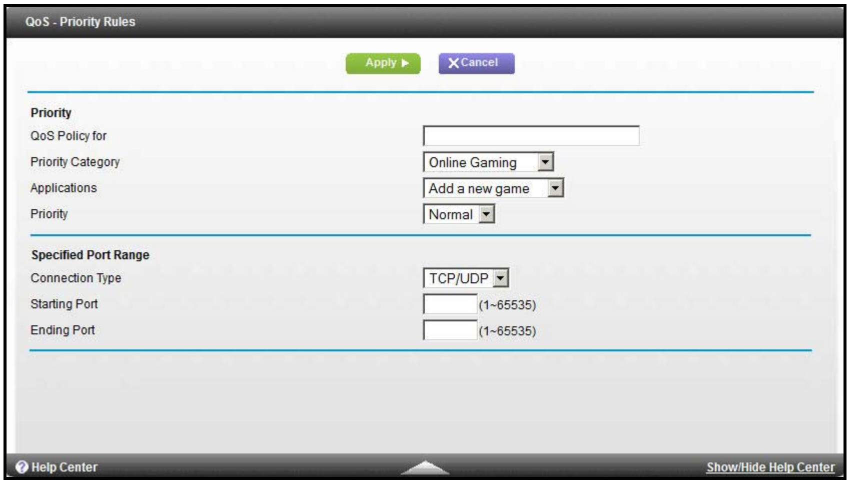
Priority: Normal

Specified Port Range

Connection Type: TCP/UDP

Starting Port: (1~65535)

Ending Port: (1~65535)



Priority

QoS Policy for

Priority Category: Online Gaming

Applications: Add a new game

Priority: Normal

Specified Port Range

Connection Type: TCP/UDP

Starting Port: (1~65535)

Ending Port: (1~65535)

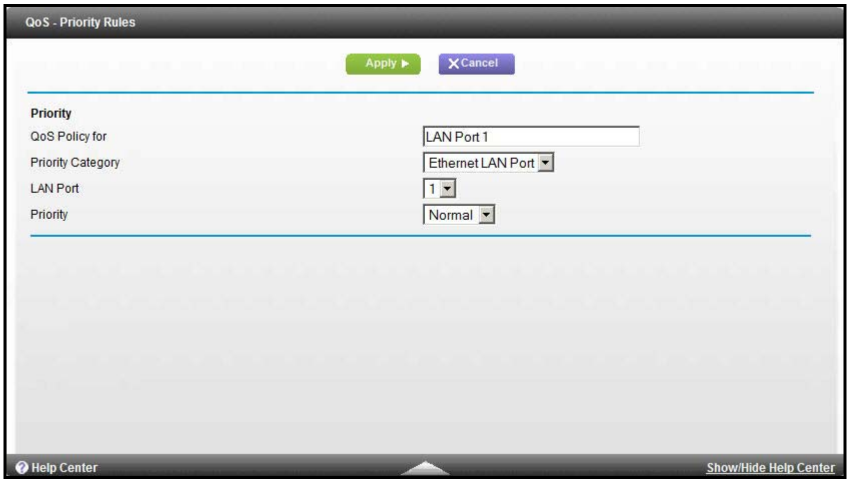
2. Select the Internet application or game from one of the lists.

3. Select the priority level: Highest, High, Normal, or Low.
4. In the QoS Policy for field, type the name for this rule.
5. Click **Apply**.

For an Ethernet LAN Port

➤ **To set up the priority for computers connected to a LAN port:**

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



Priority

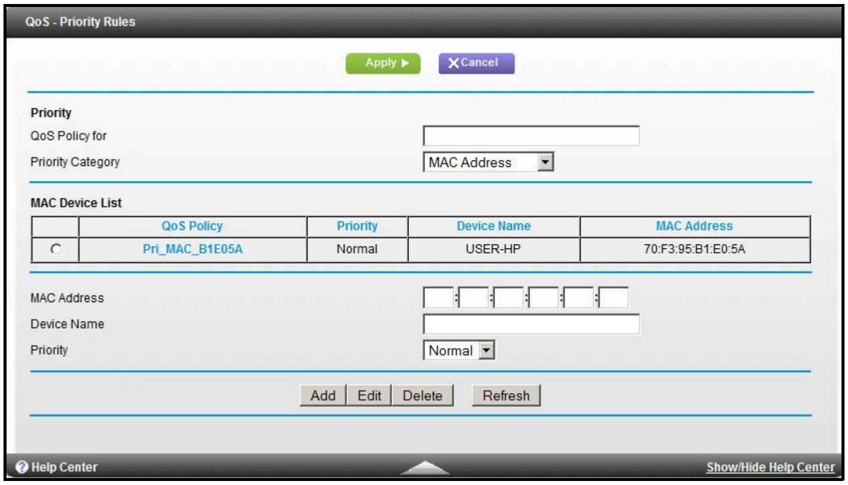
QoS Policy for	LAN Port 1
Priority Category	Ethernet LAN Port
LAN Port	1
Priority	Normal

2. Select the number of the LAN port for which you want to specify the priority level.
3. Select the priority level: Highest, High, Normal, or Low.
4. You can also type the name for this rule in the QoS Policy for field.
5. Click **Apply**.

For a MAC Address

➤ **To set up the priority for a specified computer through its MAC address:**

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



Priority

QoS Policy for	
Priority Category	MAC Address

MAC Device List

	QoS Policy	Priority	Device Name	MAC Address
○	Pri_MAC_B1E05A	Normal	USER-HP	70:F3:95:B1:E0:5A

MAC Address	: : : : :
Device Name	
Priority	Normal

2. Click **Refresh** to update the list of those computers already connected to the router.
3. Select the entry’s radio button in the table.
4. Modify the information in the MAC Address and Device Name fields.
5. Select the priority level: Highest, High, Normal, or Low.
6. You can also type the name for this rule in the QoS Policy for field.
7. Click **Edit** or **Add**.
8. Click **Apply**.

Edit or Delete an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

1. Select **ADVANCED > QoS Setup** to display the QoS Setup screen.
2. Select the radio button next to the QoS policy to edit or delete, and do one of the following:
   - Click **Delete** to remove the QoS policy.
   - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.
3. Click **Apply** in the QoS Setup screen to save your changes.

5. Security

Keeping unwanted content out of your network

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

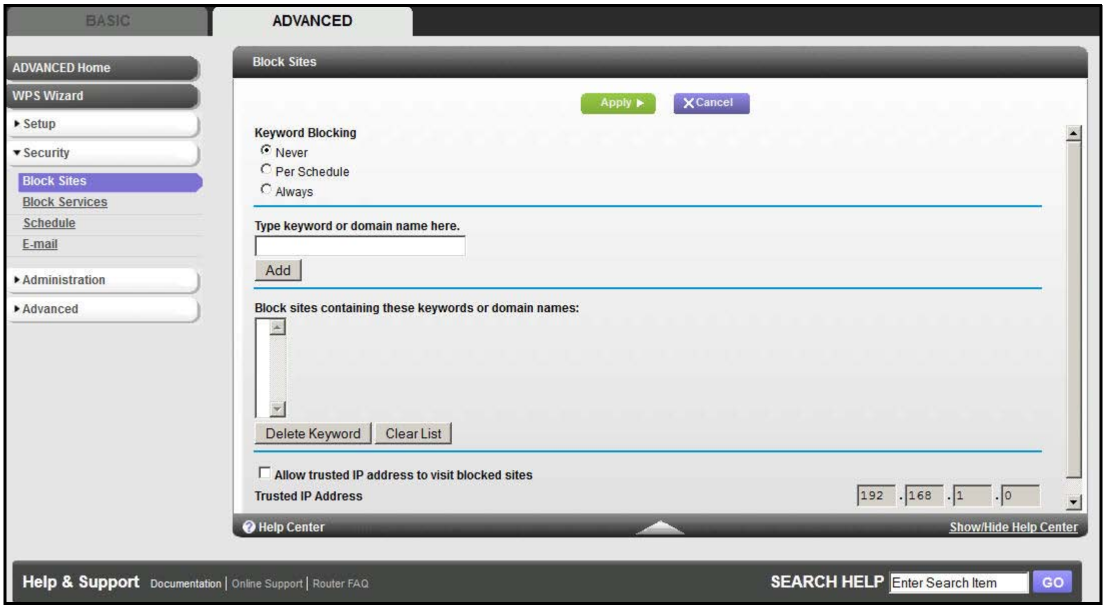
This chapter includes the following sections:

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

Keyword Blocking of HTTP Traffic

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

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



Block Sites

Keyword Blocking

● Never
○ Per Schedule
○ Always

Type keyword or domain name here.

Block sites containing these keywords or domain names:

☐ Allow trusted IP address to visit blocked sites

Trusted IP Address 192 . 168 . 1 . 0

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

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

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

➢ To delete a keyword or domain:

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

➢ 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 **Apply** to save your changes.

Block Services (Port Filtering)

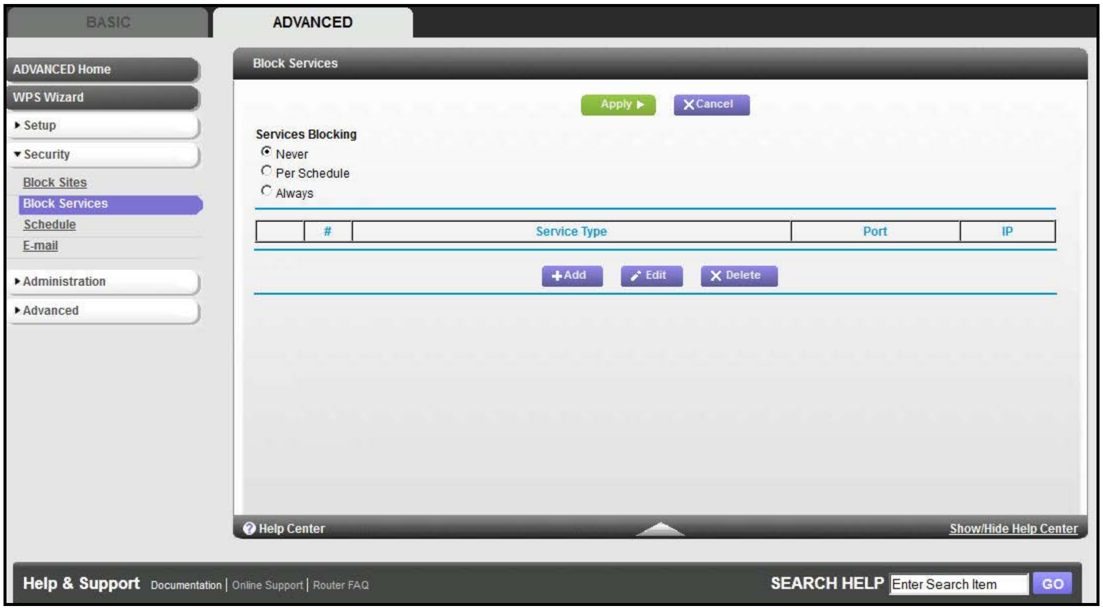
Services are functions performed by server computers at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with the destination port number 80 is an HTTP (web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024–65535 by the authors of the application. Although the 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 feature 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** to display the following screen:



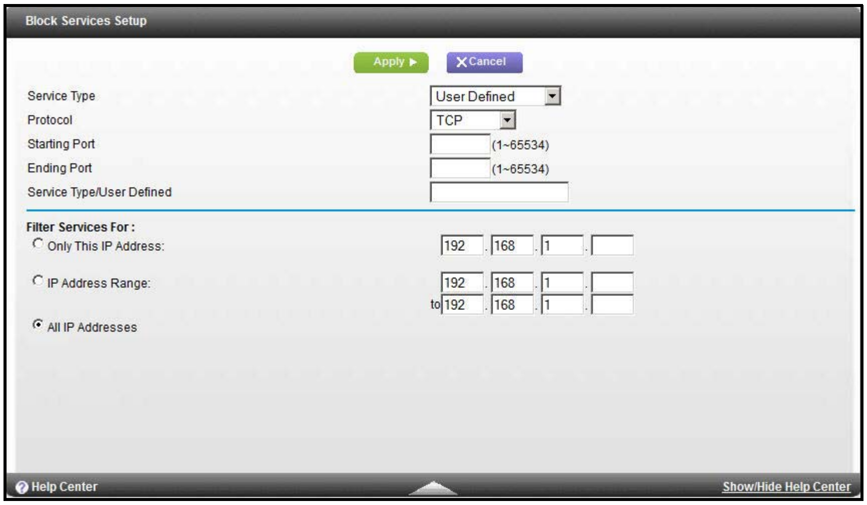
Services Blocking

● Never
○ Per Schedule
○ Always

	#	Service Type	Port	IP

2. Select either **Per Schedule** or **Always** to enable service blocking, and click **Apply**. If you selected Per Schedule, specify a time period in the Schedule screen as described in *Schedule Blocking* on page 47.

3. Click **Add** to add a service. The Block Services Setup screen displays:



Service Type: User Defined

Protocol: TCP

Starting Port: (1~65534)

Ending Port: (1~65534)

Service Type/User Defined:

Filter Services For :

○ Only This IP Address: 192 . 168 . 1 .

○ IP Address Range: 192 . 168 . 1 .
to 192 . 168 . 1 .

● All IP Addresses

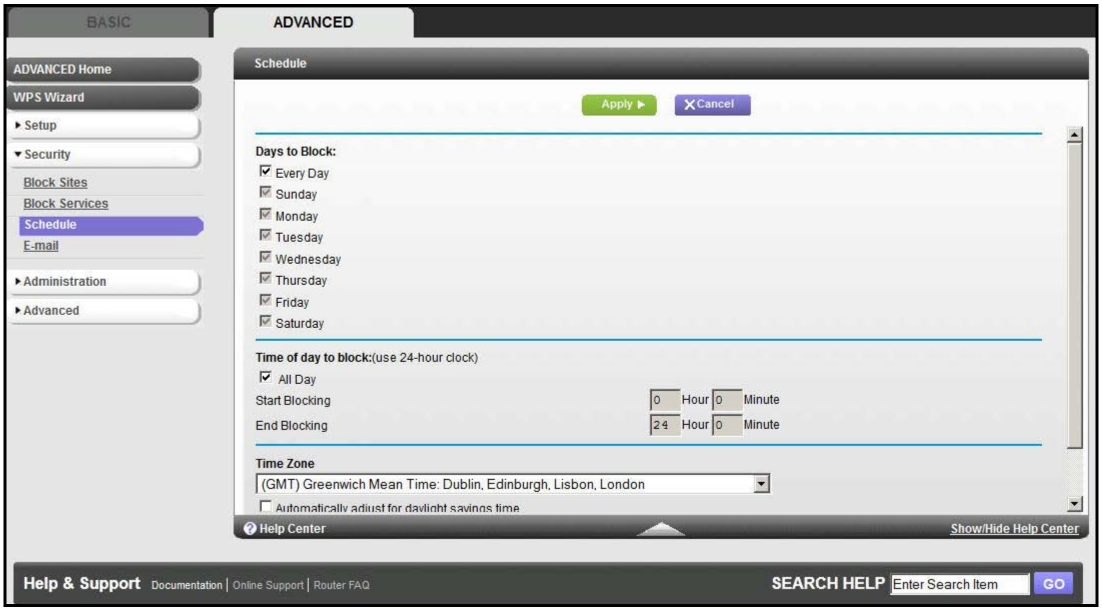
4. From the Service Type list, select the application or service to allow or block. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined.**
5. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.
6. Enter the starting and ending port numbers. If the application uses a single port number, enter that number in both fields.
7. 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.
8. Click **Add** to enable your Block Services Setup selections.

Schedule Blocking

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

➤ To schedule blocking:

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



Schedule

Days to Block:

☑ Every Day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time of day to block:(use 24-hour clock)

☑ All Day

Start Blocking 0 Hour 0 Minute

End Blocking 24 Hour 0 Minute

Time Zone

(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

□ Automatically adjust for daylight savings time

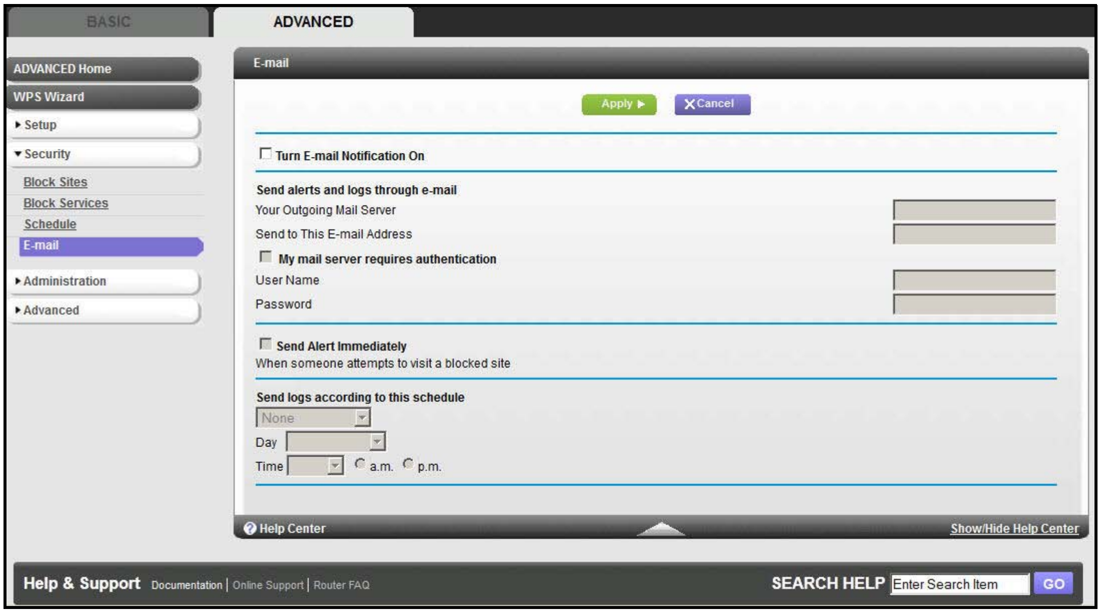
2. Set up the schedule for blocking keywords and services.
    - **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** to select the check boxes for all days.
    - **Time of day to block**. Select a start and end time in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

Security Event Email Notifications

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

➢ **To set up email notifications:**

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


BASIC
ADVANCED
ADVANCED Home
WPS Wizard
▸ Setup
▾ Security
Block Sites
Block Services
Schedule
E-mail
▸ Administration
▸ Advanced
E-mail
Apply ▸
✕ Cancel
□ Turn E-mail Notification On
Send alerts and logs through e-mail
Your Outgoing Mail Server
Send to This E-mail Address
□ My mail server requires authentication
User Name
Password
□ Send Alert Immediately
When someone attempts to visit a blocked site
Send logs according to this schedule
None
Day
Time
○ a.m. ○ p.m.
Help Center
Show/Hide Help Center
Help & Support Documentation | Online Support | Router FAQ
SEARCH HELP
Enter Search Item
GO

2. To receive email logs and alerts from the router, select the **Turn E-mail Notification On** check box.
3. In the Your Outgoing Mail Server field, enter the name of your ISP outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration screen of your email program. When you leave this field blank, log and alert messages do not get sent by email.
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. When you leave this field blank, log and alert messages do not get sent by email.
5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.
6. You can have email alerts sent immediately when someone attempts to visit a blocked site, and you can specify that logs are sent automatically.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, the log is cleared from the router’s 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.
7. Click **Apply** to save your settings.

6. Administration

Managing your network

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

- See *Attached Devices* on page 23 to view all computers or devices that are currently connected to your network.
- See *Remote Management* on page 79 for information about upgrading or checking the status of your router over the Internet.
- See *Traffic Meter* on page 82 for information about monitoring the volume of Internet traffic passing through your router’s Internet port.

This chapter includes the following sections:

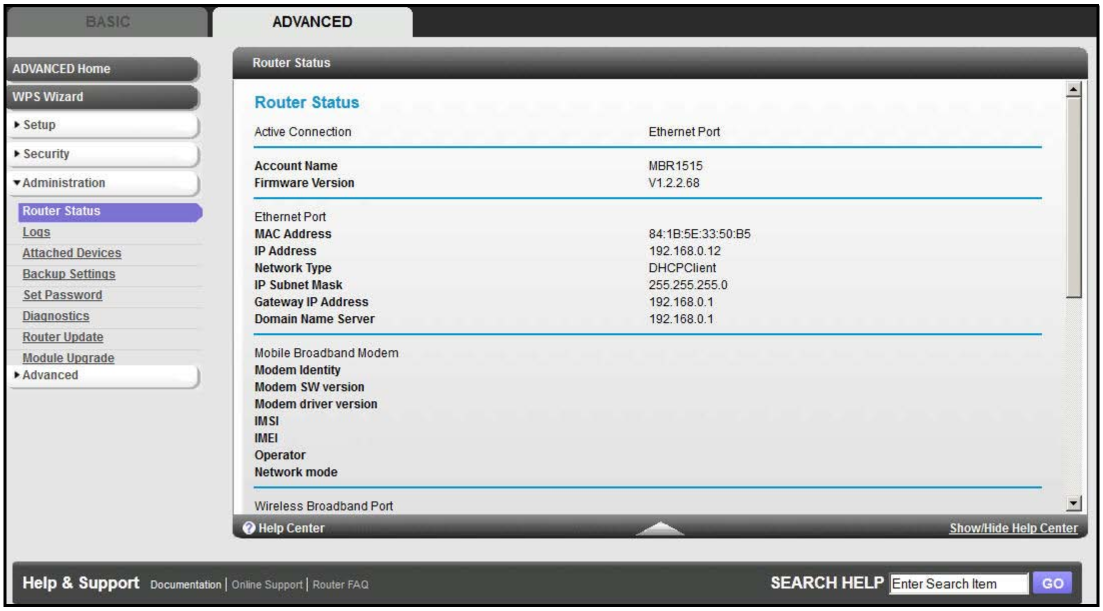
- *Router Status*
- *Logs*
- *Backup Settings*
- *Set Password*
- *Diagnostics*
- *Router Upgrade*
- *Module Upgrade*

Router Status

Use the Router Status screen to check the current settings and statistics for your router. This screen shows you the current settings. If something needs to be changed, change it on the relevant screen.

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

1. Select **ADVANCED > Administration > Router Status** to display the following screen:



Router Status

Active Connection Ethernet Port

Account Name MBR1515
Firmware Version V1.2.2.68

Ethernet Port
MAC Address 84:1B:5E:33:50:B5
IP Address 192.168.0.12
Network Type DHCPClient
IP Subnet Mask 255.255.255.0
Gateway IP Address 192.168.0.1
Domain Name Server 192.168.0.1

Mobile Broadband Modem
Modem Identity
Modem SW version
Modem driver version
IMSI
IMEI
Operator
Network mode

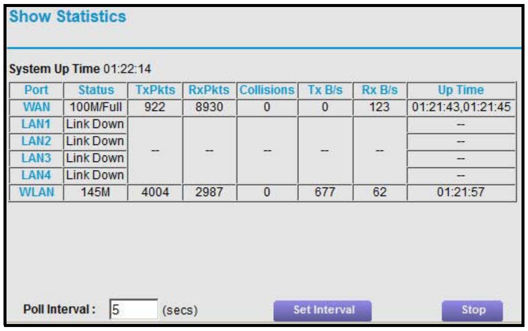
Wireless Broadband Port

The following status information is displayed:

- **Active Connection**. The current WAN interface used by the router.
- **Account Version**. The router model.
- **Firmware Version**. The version of the router firmware. It changes if you upgrade the router firmware.
- **Ethernet Port**. The current settings of Ethernet broadband port.
  - **MAC Address**. The Media Access Control address. This address is the unique physical address used by the Ethernet (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, the router cannot connect to the Internet.
  - **Network Type**. 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.
  - **Gateway IP Address**. The IP address used by 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.
- **Mobile Broadband Modem**. This section shows the properties of the mobile broadband modem.
  - **Modem Identity**. Shows the modem in use.
  - **Modem SW version**. The software version of the modem.
  - **Modem driver version**. The driver version of the modem.
  - **IMEI**. International Mobile Equipment Identity. The unique identity of the modem.
  - **Operator**. The ISP for the broadband wireless network.
  - **Network mode**. The mode of the current network the modem is connected to. This mode is dependent on coverage and distance from the cell site.
- **Wireless Broadband Port**. The current settings of mobile broadband port.
  - **Connection Status**. This setting shows the status of the wireless broadband connection.
  - **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, the router cannot connect to the Internet.
  - **Protocol**. 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.
- **LAN Port**. These values are the current settings, as set in the LAN Setup screen.
  - **MAC Address**. The Media Access Control address. This address 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 192.168.0.1.
  - **DHCP**. Identifies whether the router’s built-in DHCP server is active for the LAN-attached devices.
  - **IP Subnet Mask**. The subnet mask associated with the LAN IP address.
- **Wireless Port**. These values are the current settings, as set in the Wireless Settings screen.
  - **Name (SSID)**. The SSID of the router.
  - **Region**. The location (country).
  - **Channel**. The current channel in use.
  - **Wireless AP**. Indicates if the access point feature of the router is enabled or not. If not enabled, the WiFi LED on the front panel is off.
  - **Broadcast Name**. Indicates if the router is broadcasting its SSID.

2. Click **Show Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port.



Show Statistics

System Up Time 01:22:14

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	922	8930	0	0	123	01:21:43,01:21:45
LAN1	Link Down	--	--	--	--	--	--
LAN2	Link Down						--
LAN3	Link Down						--
LAN4	Link Down						--
WLAN	145M	4004	2987	0	677	62	01:21:57

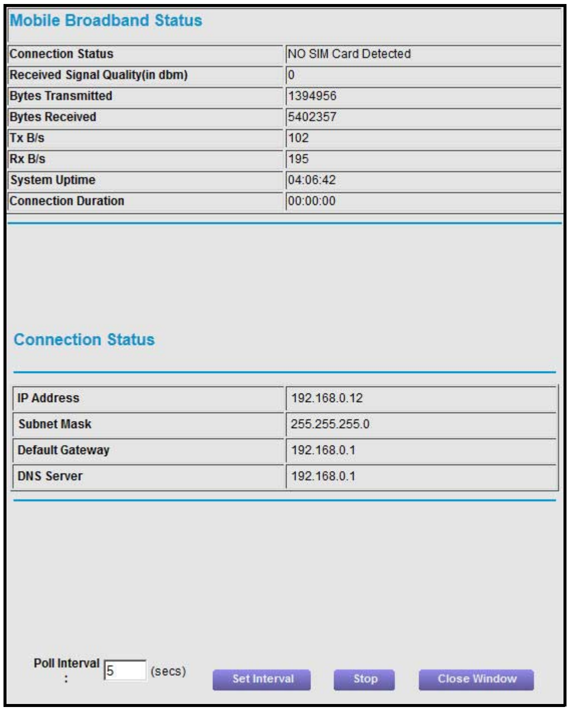
Poll Interval : 5 (secs)

- **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 **Set Interval**.

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

3. Click **Connection Status** to see information about your current connection.



Mobile Broadband Status

Connection Status	NO SIM Card Detected
Received Signal Quality(in dbm)	0
Bytes Transmitted	1394956
Bytes Received	5402357
Tx B/s	102
Rx B/s	195
System Uptime	04:06:42
Connection Duration	00:00:00

Connection Status

IP Address	192.168.0.12
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DNS Server	192.168.0.1

Poll Interval : 5 (secs)

- Mobile Broadband Status.
  - **Connection Status**. The status of the Internet connection.
  - **Received Signal Quality (in dBm)**. Modem radio reception. A small, negative number indicates good signal quality.
  - **Bytes Transmitted**. The number of bytes transmitted in the most recent connection session.
  - **Bytes Received**. The number of bytes received in the most recent connection session.
  - **Tx B/s**. The transmission rate.
  - **Rx B/s**. The receiving rate.
  - **System Uptime**. Time elapsed since the last reboot.
  - **Connection Duration**. Length of the current connection.
- Connection Status.
  - **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.
  - **DNS Server**. The IP address of the Domain Name Service server that provides translation of network names to IP addresses.

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

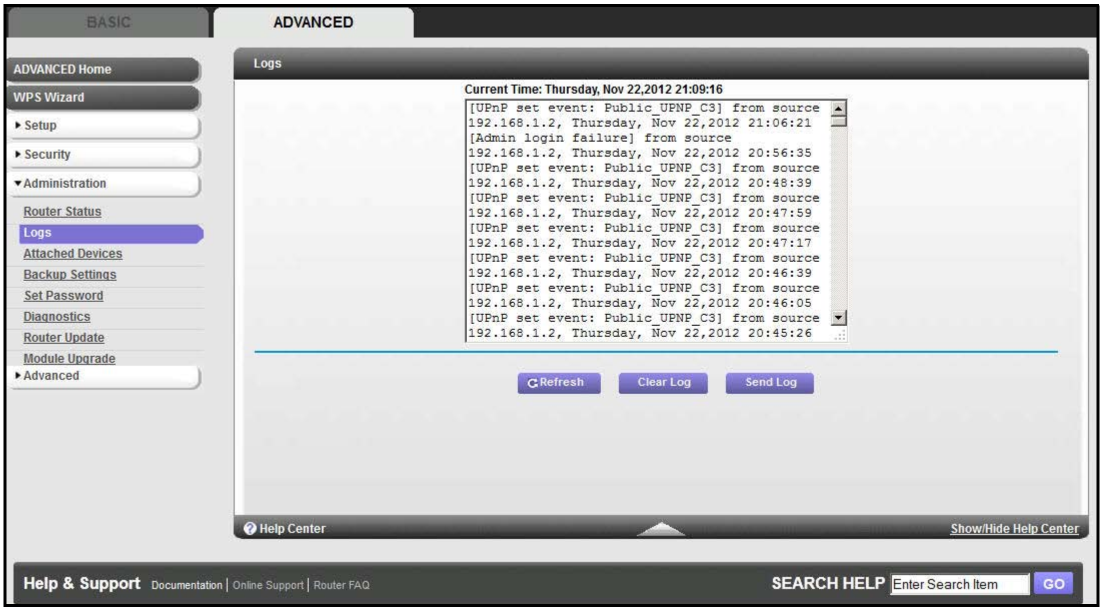
To stop the polling entirely, click **Stop**.

The Close Window button closes the Connection Status screen.

Logs

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

Select **ADVANCED > Administration > Logs**. The Logs screen displays.



Current Time: Thursday, Nov 22,2012 21:09:16

```
[UPnP set event: Public_UPNP_C3] from source
192.168.1.2, Thursday, Nov 22,2012 21:06:21
[Admin login failure] from source
192.168.1.2, Thursday, Nov 22,2012 20:56:35
[UPnP set event: Public_UPNP_C3] from source
192.168.1.2, Thursday, Nov 22,2012 20:48:39
[UPnP set event: Public_UPNP_C3] from source
192.168.1.2, Thursday, Nov 22,2012 20:47:59
[UPnP set event: Public_UPNP_C3] from source
192.168.1.2, Thursday, Nov 22,2012 20:47:17
[UPnP set event: Public_UPNP_C3] from source
192.168.1.2, Thursday, Nov 22,2012 20:46:39
[UPnP set event: Public_UPNP_C3] from source
192.168.1.2, Thursday, Nov 22,2012 20:46:05
[UPnP set event: Public_UPNP_C3] from source
192.168.1.2, Thursday, Nov 22,2012 20:45:26
```

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. This feature can be useful for testing your email settings.

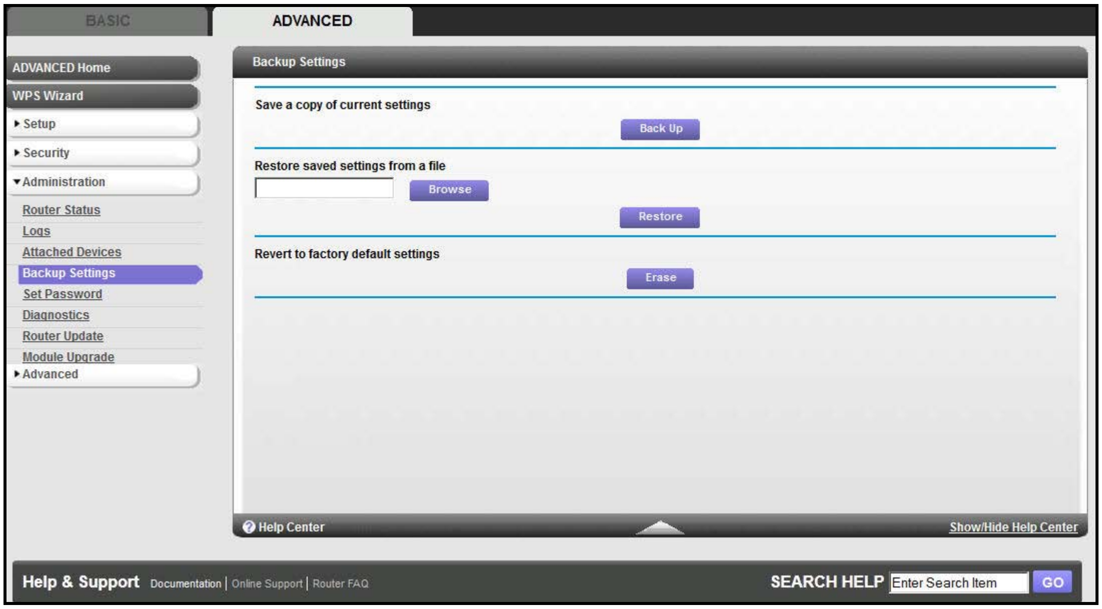
Backup Settings

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** to display the following screen:



2. Click **Back Up** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore Configuration Settings

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

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

When the restoration is complete, the router reboots.

WARNING:

Do not interrupt the reboot process.

Erase

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

You can either use the Restore Factory Settings button on the back of the router (see *Factory Default Settings* on page 93), or you can click the **Erase** button in this screen.

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

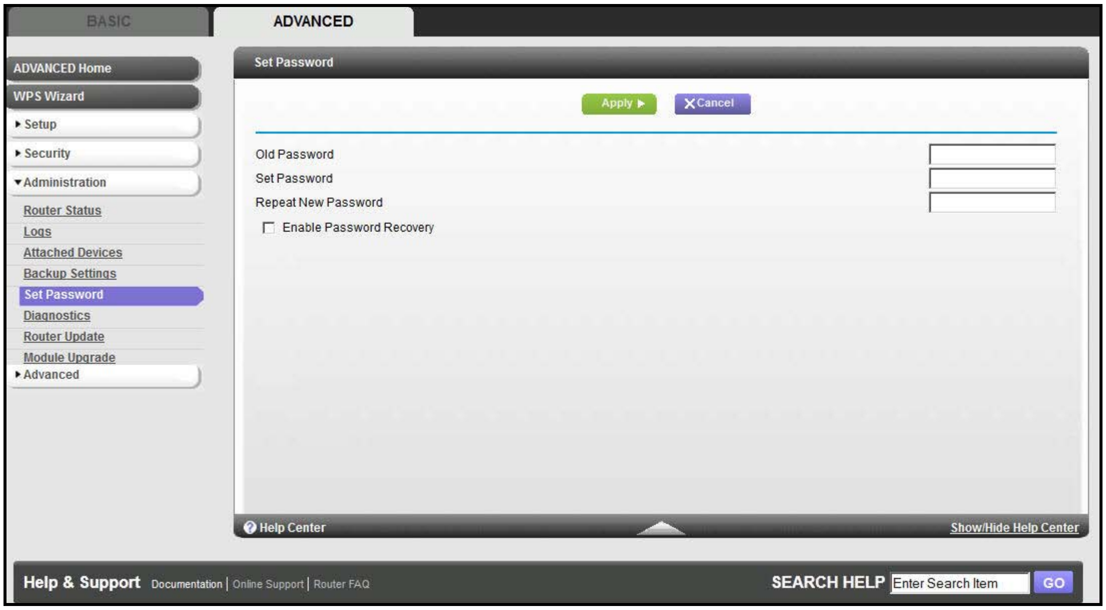
Set Password

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

This change of password is not the same as changing the password for wireless access. The label on the bottom of your router shows your unique wireless network name (SSID) and password for wireless access (see *Router Label* on page 10).

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

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



2. Type the old password, and type the new password twice in the fields on this screen.
3. If you want to be able to recover the password, select the **Enable Password Recovery** check box.
4. Click **Apply** so that your changes take effect.

Password Recovery

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

➤ To set up password recovery:

1. Select the **Enable Password Recovery** check box.
2. Select two security questions, and provide answers to them.
3. Click **Apply** to save your changes.

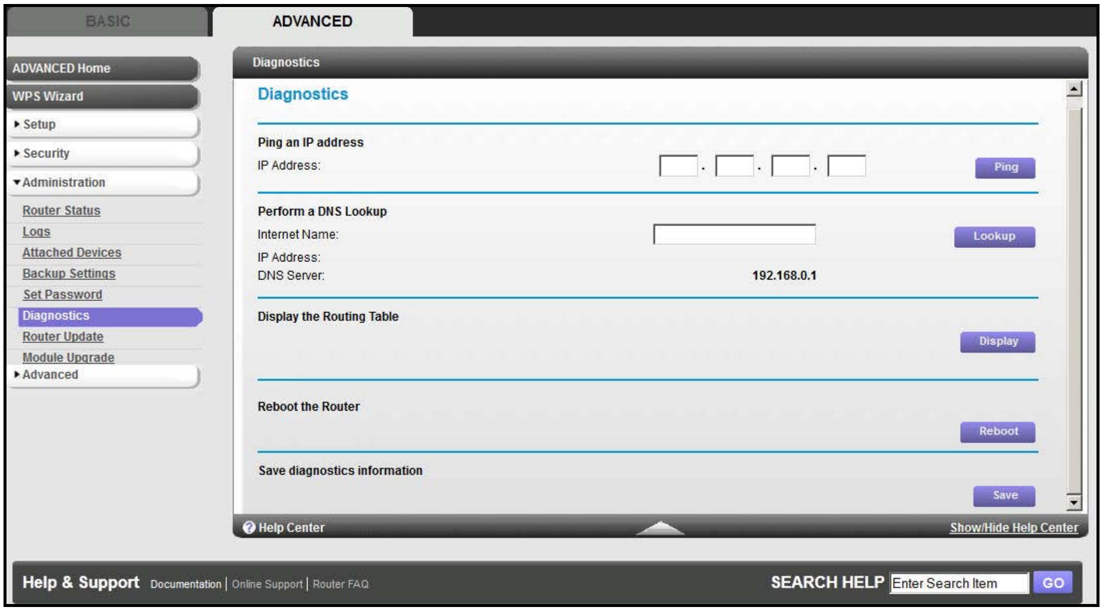
When you use your browser to access the router, the login screen displays. If password recovery is enabled, when you click Cancel, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

Diagnostics

Use the Diagnostics screen to perform various diagnostics. For normal operation, these tests are not required.

➤ To run the diagnostics:

Select **ADVANCED > Administration > Diagnostics** to display the following screen:



DNS Server: 192.168.0.1

Ping an IP address. Use this test to send a ping packet request to the specified IP address. This procedure is often used to test a connection. If the request times out because no reply is received, this result usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping.

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

Display the Routing Table. This operation displays the internal routing table. This information gets used by technical support and other staff who understand routing tables.

Reboot the Router. Use this button to perform a remote reboot (restart). You can use this procedure when the router seems to have become unstable or is not operating normally.

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

Save diagnostics information. Use this button to view the diagnostics information.

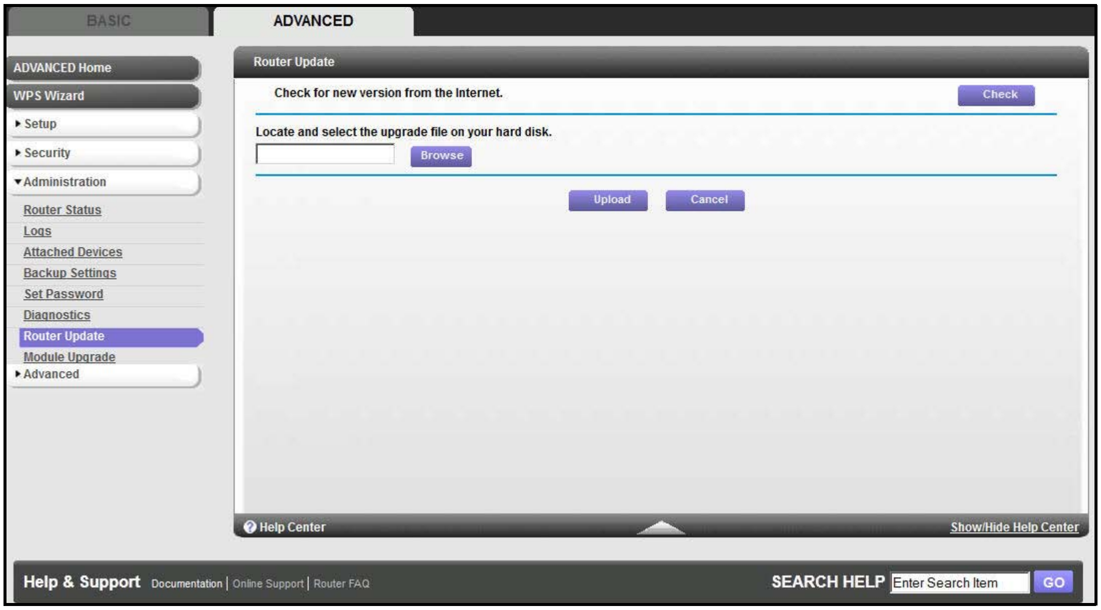
Router Upgrade

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 NETGEAR genie screens when new firmware is available for your product.

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

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

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



Check for new version from the Internet.

Locate and select the upgrade file on your hard disk.

2. Click **Check**.

   The router finds new firmware information if any is available.

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

WARNING:

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

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

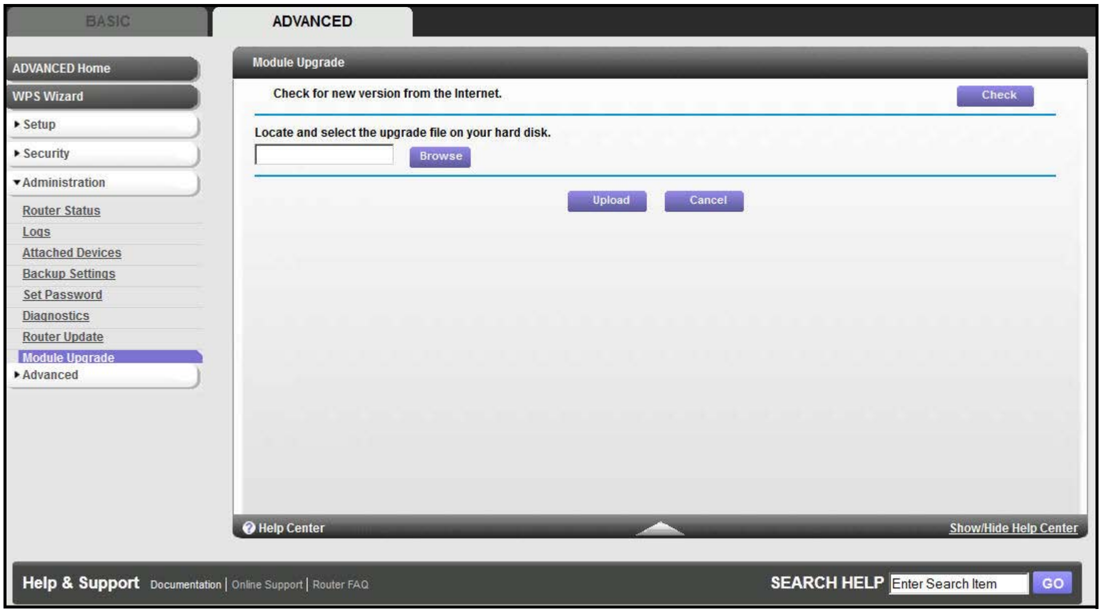
Module Upgrade

The module firmware (broadband mobile software) is stored in flash memory. You can upgrade the firmware from the Administration menu on the ADVANCED tab. You might see a message at the top of the NETGEAR genie screens when new firmware is available for your product.

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

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

1. Select **ADVANCED > Administration > Module Upgrade** to display the following screen:



Module Upgrade

Check for new version from the Internet.

Locate and select the upgrade file on your hard disk.

2. Click **Check**.

   The router finds new firmware information if any is available.

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

⚠ WARNING:

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

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

Advanced Settings

7

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

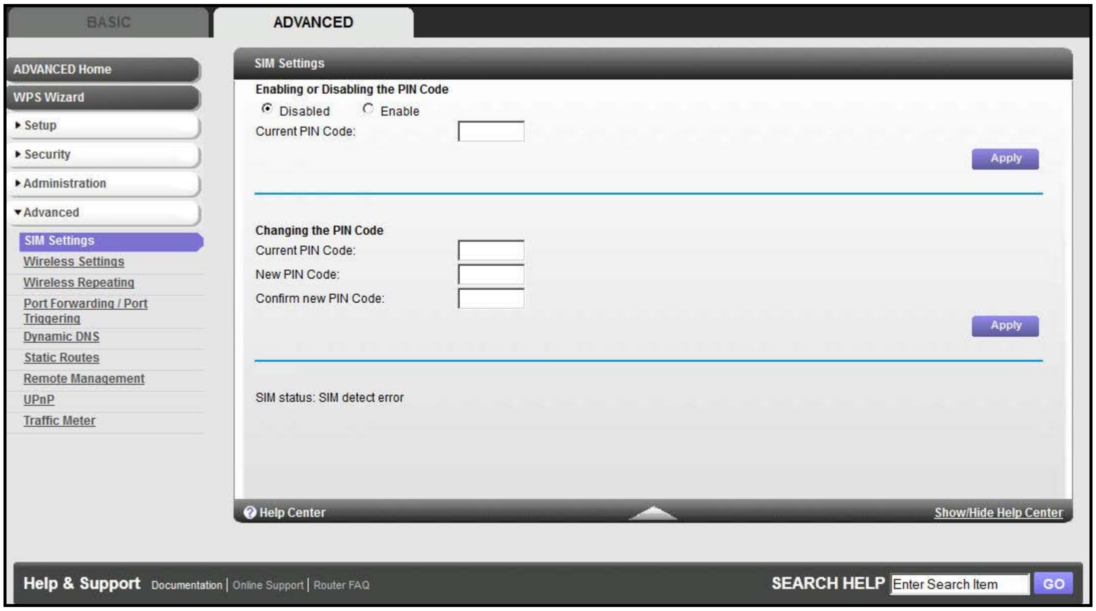
This chapter includes the following sections:

SIM Settings

Your ISP provides you with a SIM card so that you can access mobile broadband. Use this screen to change your SIM card settings.

➤ **To change your SIM card settings:**

1. Select **ADVANCED > Advanced > SIM Settings** to display the following screen:



SIM Settings

Enabling or Disabling the PIN Code

● Disabled ○ Enable

Current PIN Code:

Changing the PIN Code

Current PIN Code:

New PIN Code:

Confirm new PIN Code:

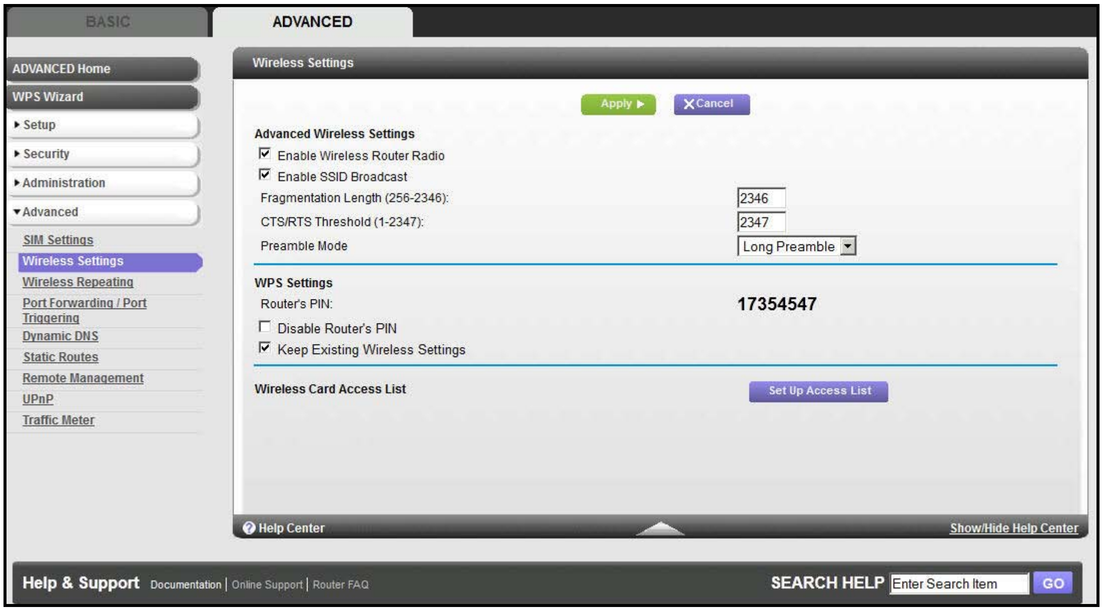
SIM status: SIM detect error

2. Change your SIM card settings as necessary:
   - **Enabling or Disabling the PIN Code**. Enable or disable the use of the SIM card PIN code. Enter your current PIN code to authorize this change.
   - **Changing the PIN Code**. The PIN code prevents the use of the SIM card in an unauthorized device. Also, change the PIN code regularly for security reasons. Enter your current PIN code to authorize this change, followed by the new PIN code you have chosen.
3. Click **Appl**y so that your changes take effect.

Wireless Settings

Note: The wireless router is already configured with the optimum settings. Do not alter these settings unless directed by NETGEAR support. Incorrect settings disable the wireless router.

Select **ADVANCED > Advanced > Wireless Settings** to display the following screen:



Wireless Settings

Advanced Wireless Settings

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

Fragmentation Length (256-2346): 2346

CTS/RTS Threshold (1-2347): 2347

Preamble Mode: Long Preamble

WPS Settings

Router's PIN: 17354547

☐ Disable Router's PIN

☑ Keep Existing Wireless Settings

Wireless Card Access List

The following settings are available in this screen:

Advanced Wireless Settings. Do not change these settings unless directed to do so by NETGEAR support.

- **Enable Wireless Router Radio**. You can completely turn off the wireless portion of the wireless router by clearing this check box. Select this check box again to enable the wireless portion of the router. When the wireless radio is disabled, other members of your household can use the router by connecting their computers to the router with an Ethernet cable.
- **Enable SSID Broadcast**. This setting enables broadcasting of the SSID.

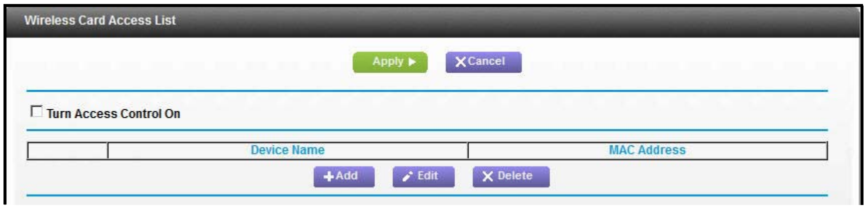
Note: The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

WPS Settings.You can add WPS devices to your network.

- **Router’s PIN**. This PIN is the PIN number you use on a registrar (such as from Network Explorer on a Vista Windows computer) to configure the router’s wireless settings through WPS. You can also find the PIN on the router’s product label.
- **Disable Router’s PIN**. You can configure the router’s wireless settings or add a wireless client through WPS using the router’s PIN only when the PIN is enabled. The router’s PIN can be disabled temporarily 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 this function by clearing the check box and clicking the Apply button.
- **Keep Existing Wireless Settings**. This setting shows whether the router is in the WPS configured state. If this option is not selected, adding a new wireless client changes the router’s wireless settings to an automatically generated random SSID and security key. In addition, when this option is selected, some external registrars (such as Network Explorer on Vista Windows) might not see the router.

  Configuring the basic wireless settings from the router’s web management interface selects this option automatically.

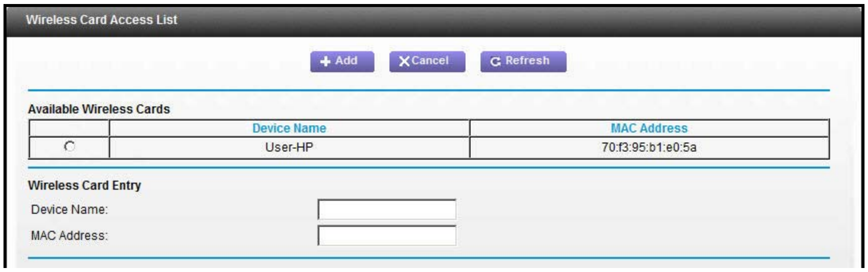
Wireless Card Access List. By default, any wireless computer that is configured with the correct SSID is allowed access to your wireless network. For increased security, restrict access to the wireless network to allow only specific computers based on their MAC addresses. Click the **Set Up Access List** button display the Wireless Card Access List screen. On this screen, you can restrict access to your network to specific devices based on their MAC address.



□ Turn Access Control On

	Device Name	MAC Address

Click **Add** to add wireless devices to your network based on their MAC addresses.



Available Wireless Cards

	Device Name	MAC Address
○	User-HP	70:f3:95:b1:e0:5a

Wireless Card Entry

Device Name:

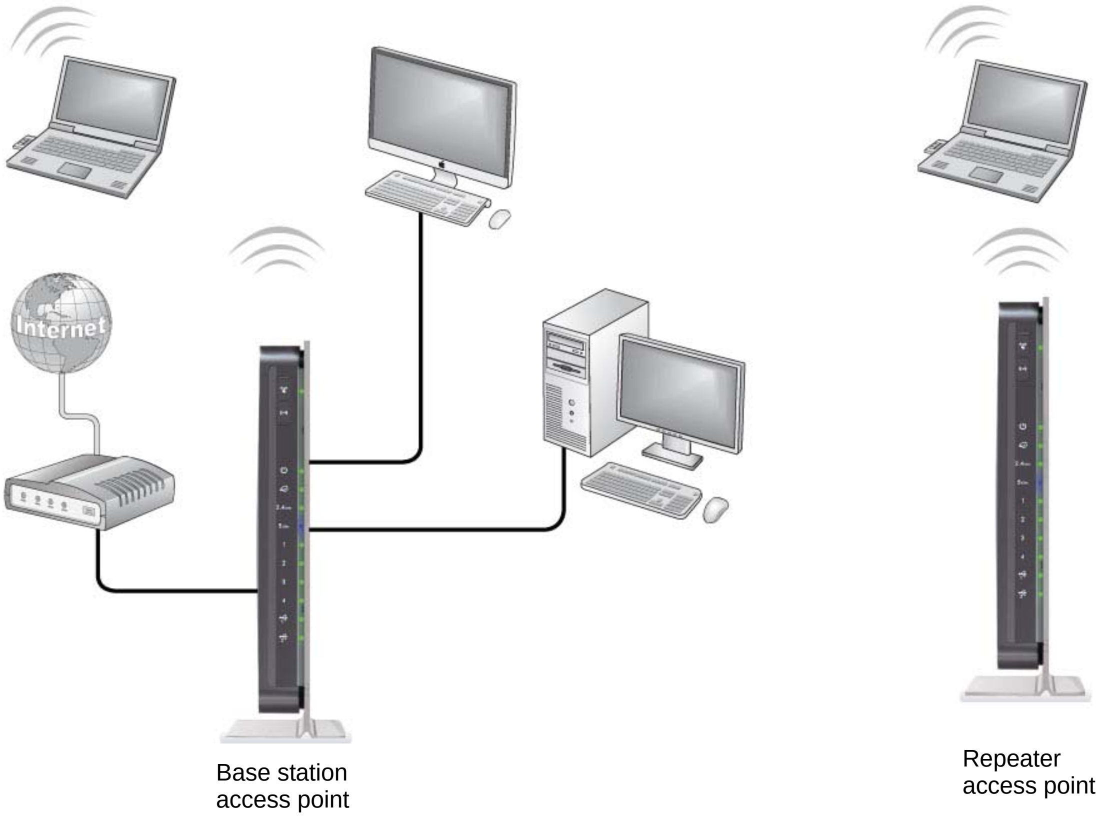
MAC Address:

Click **Apply** to have your changes take effect.

Wireless Repeating

You can set the router up to be used as a wireless access point (AP). This setup enables the router to act as a wireless repeater. A wireless repeater connects to another wireless router as a client where the network to which it connects becomes the ISP service.

Wireless repeating is a type of Wireless Distribution System (WDS). A WDS allows a wireless network to be expanded through multiple access points instead of using a wired backbone to link them. The following figure shows a wireless repeating scenario.



Note: If you use the wireless repeating function, you need to select either **WEP** or **None** as a security option in the Wireless Settings screen. The WEP option displays only if you select the wireless mode Up to 54 Mbps in the Wireless Settings screen.

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

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

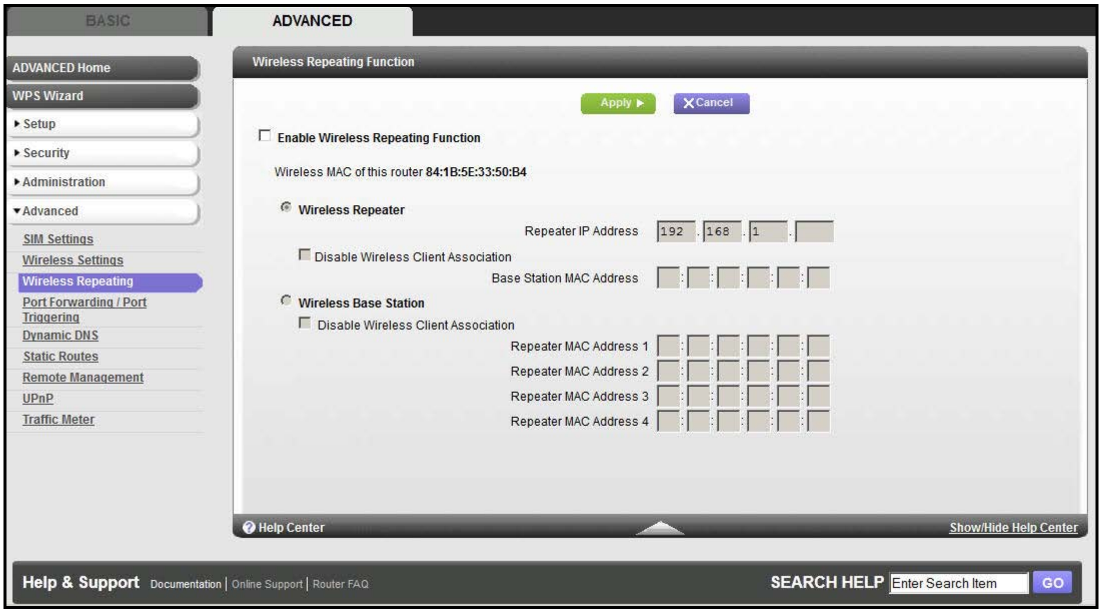
The MBR1515 router is always in dual-band concurrent mode, unless you turn off one radio. When you enable the wireless repeater in either radio band, the wireless base station, or wireless repeater, cannot be enabled in the other radio band. However, if you enable the wireless base station in either 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, the following conditions have to be met for both access points:

- 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 the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) have to be configured to operate in the same LAN network address range as the access points.

Wireless Repeating Function

Select **ADVANCED > Advanced > Wireless Repeating** to view or change wireless repeater settings for the router.



Wireless Repeating Function

□ Enable Wireless Repeating Function

Wireless MAC of this router 84:1B:5E:33:50:B4

● Wireless Repeater

Repeater IP Address 192 . 168 . 1 .

□ Disable Wireless Client Association

Base Station MAC Address

○ Wireless Base Station

□ Disable Wireless Client Association

Repeater MAC Address 1

Repeater MAC Address 2

Repeater MAC Address 3

Repeater MAC Address 4

- **Enable Wireless Repeating Function**. Select the check box for the 2.4 GHz or 5 GHz network to use the wireless repeating function.
- **Wireless MAC of this router**. This field displays the MAC address for your router for your reference. You need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.
- **Wireless Repeater**. If your router is the repeater, select this radio button.

Repeater IP Address. If your router is the repeater, enter the IP address of the other access point.

Disable Wireless Client Association. If your router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

- If you are setting up a point-to-point bridge, select this check box.
- If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

Base Station MAC Address. If your router is the repeater, enter the MAC address for the access point that is the base station.

- **Wireless Base Station**. If your router is the base station, select this radio button.

  Disable Wireless Client Association. If your router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

  Repeater MAC Address (1 through 4). If your router is the base station, it can act as the “parent” of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

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 and then set up the repeater.

➢ **To set up the base station:**

1. Set up both units with the same wireless settings (SSID, mode, channel, and security). The wireless security option has to be set to None or WEP.
2. Select **ADVANCED > Advanced > Wireless Repeating Function** to display the Wireless Repeating Function screen.
3. In the Wireless Repeating Function screen (depending on the frequency you want to use), select the **Enable Wireless Repeating Function** check box and select the **Wireless Base Station** radio button.
4. Enter the MAC address for one or more repeater units.
5. Click **Apply** to save your changes.

Set Up a Repeater Unit

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 MBR1515 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 wireless repeater AP.

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

1. Log in to the router that is to be the repeater. 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**.
2. Select **ADVANCED > Advanced > Wireless Repeating Function**. Select the **Enable Wireless Repeating Function** check box and the **Wireless Repeater** radio button.
3. 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.
4. Click **Apply** to save your changes.
5. Verify connectivity across the LANs.

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

Port Forwarding and Port Triggering

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

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when their replies do not get recognized by your router.

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

Remote Computer Access Basics

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

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

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type http://www.example.com into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your router.

   Source address. Your computer’s IP address.

   Source port number. 5678, which is the browser session.

   Destination address. The IP address of www.example.com, which your computer finds by asking a DNS server.

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

   Your router then sends this request message through the Internet to the web server at www.example.com.
4. The web server at www.example.com composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your router.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. The public IP address of your router.

   Destination port number. 33333.
5. Upon receiving the incoming message, your router checks its session table to determine whether an active session for port number 33333 exists. Finding an active session, the router then modifies the message to restore the original address information replaced by NAT. Your router sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. Your computer’s IP address.

Destination port number. 5678, which is the browser session that made the initial request.

6. When you finish your browser session, your router eventually detects a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Port Triggering to Open Incoming Ports

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

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an “identify” message to your computer on port 113. Using port triggering, you can tell the router, “When you initiate a session with destination port 6667, you 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 (as in the previous example, say port 33333) as the destination port. The IRC server also sends an “identify” message to your router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether an active session for port number 33333 exists. 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 learns that an active session for port 113 exists and is 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 triggers the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

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

Port Forwarding to Permit External Host Communications

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

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser 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 determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

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

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

Set Up Port Forwarding to Local Servers

Using the port forwarding feature, you can 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.

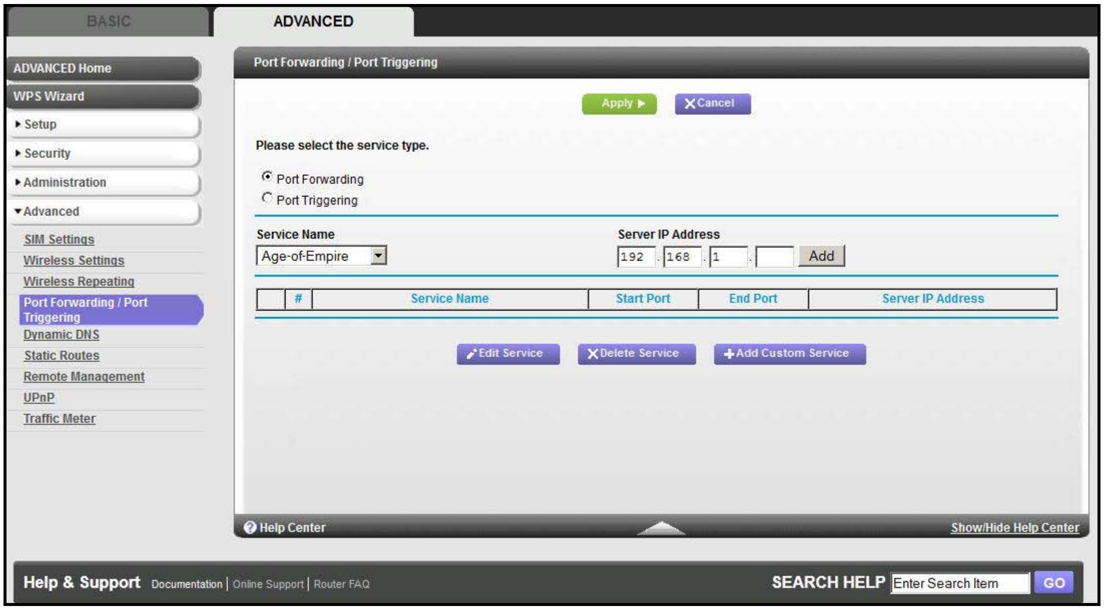
Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

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

➢ **To set up port forwarding:**

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your router.

1. Select **ADVANCED > Advanced > Port Forwarding/Port Triggering** to display the following screen:



Please select the service type.

● Port Forwarding
○ Port Triggering

Service Name: Age-of-Empire

Server IP Address: 192 . 168 . 1 .

	#	Service Name	Start Port	End Port	Server IP Address

Port Forwarding is selected as the service type.

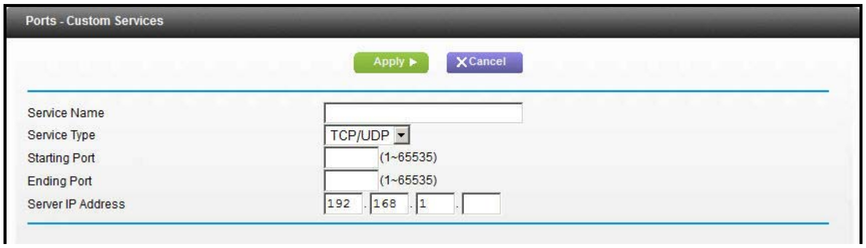
2. From the Service Name list, select the service or game that you host on your network. If the service does not appear in the list, see *Add a Custom Service* on page 73.
3. In the corresponding Server IP Address field, enter the last digit of the IP address of your local computer that provides this service.
4. Click **Add**. The service appears in the list in the screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you have to first determine which port number or range of numbers gets used by the application. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➢ To add a custom service:

1. Select **ADVANCED > Advanced > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.
3. Click the **Add Custom Service** button to display the following screen:



Service Name	
Service Type	TCP/UDP
Starting Port	(1~65535)
Ending Port	(1~65535)
Server IP Address	192 . 168 . 1 .

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

5. In the Service Type list, select the protocol. If you are unsure, select **TCP/UDP**.
6. In the Starting Port field, enter the beginning port number.
   - If the application uses a single port, enter the same port number in the Ending Port field.
   - If the application uses a range of ports, enter the ending port number of the range in the Ending Port field.
7. In the Server IP Address field, enter the IP address of your local computer that provides this service.
8. Click **Apply**. 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. In the table, select the radio button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Making 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 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 as described in *Dynamic DNS* on page 76. To access your web server from the Internet, a remote user has to know the IP address that your ISP assigns. 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.

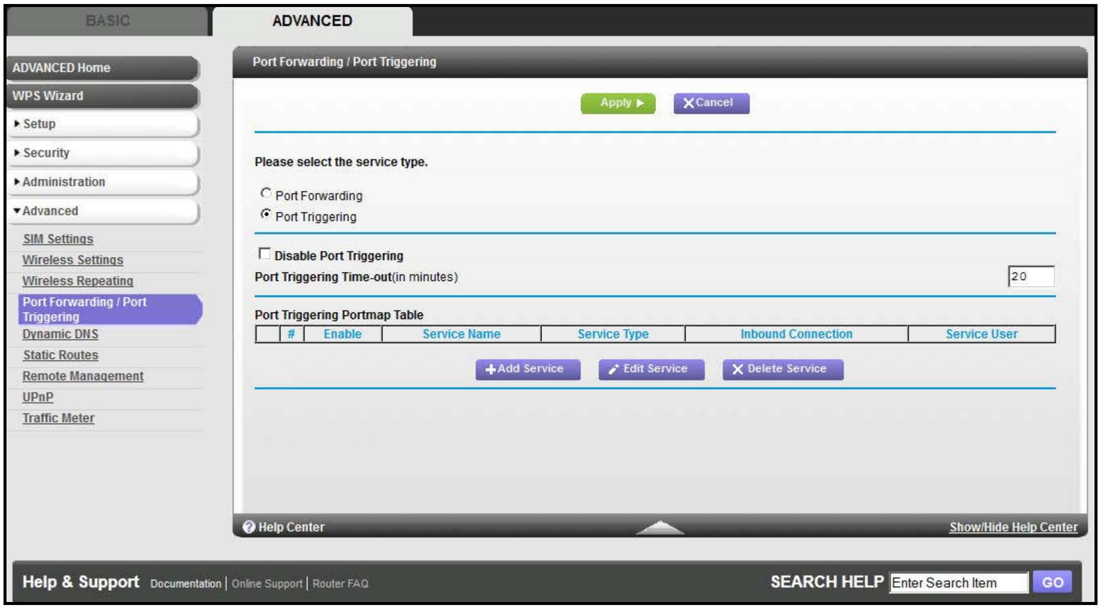
Port forwarding creates a static mapping of a port number or range to a single local computer. Port triggering, on the other hand, can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 81.

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

➤ **To set up port triggering:**

1. Select **ADVANCED > Advanced > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button to display the port triggering information.



Please select the service type.

○ Port Forwarding
● Port Triggering

☐ Disable Port Triggering

Port Triggering Time-out(in minutes) 20

Port Triggering Portmap Table

	#	Enable	Service Name	Service Type	Inbound Connection	Service User

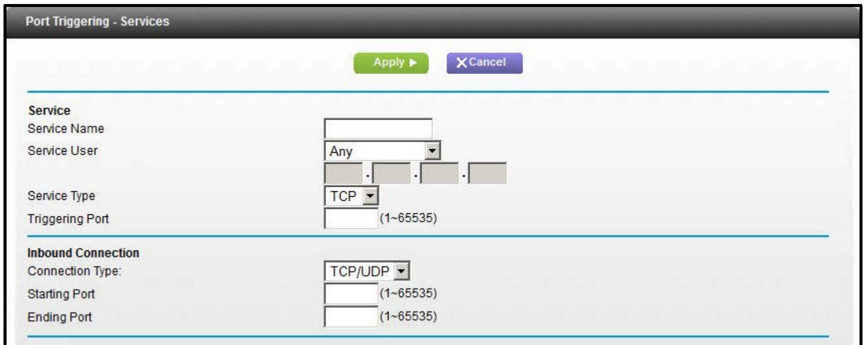
3. Clear the **Disable Port Triggering** check box if it is selected.

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

4. In the Port Triggering Timeout 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. This value is required because the router cannot be sure when the application has terminated.

5. Click **Add Service** to display the following screen:



Service

Service Name	
Service User	Any
	. . .
Service Type	TCP
Triggering Port	(1~65535)

Inbound Connection

Connection Type:	TCP/UDP
Starting Port	(1~65535)
Ending Port	(1~65535)

6. In the Service Name field, type a descriptive service name.
7. In the Service User list, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.
8. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.
9. In the Triggering Port field, enter the number of the outbound traffic port that causes the inbound ports to open.
10. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
11. Click **Apply**. The service appears in the Port Triggering Portmap table.

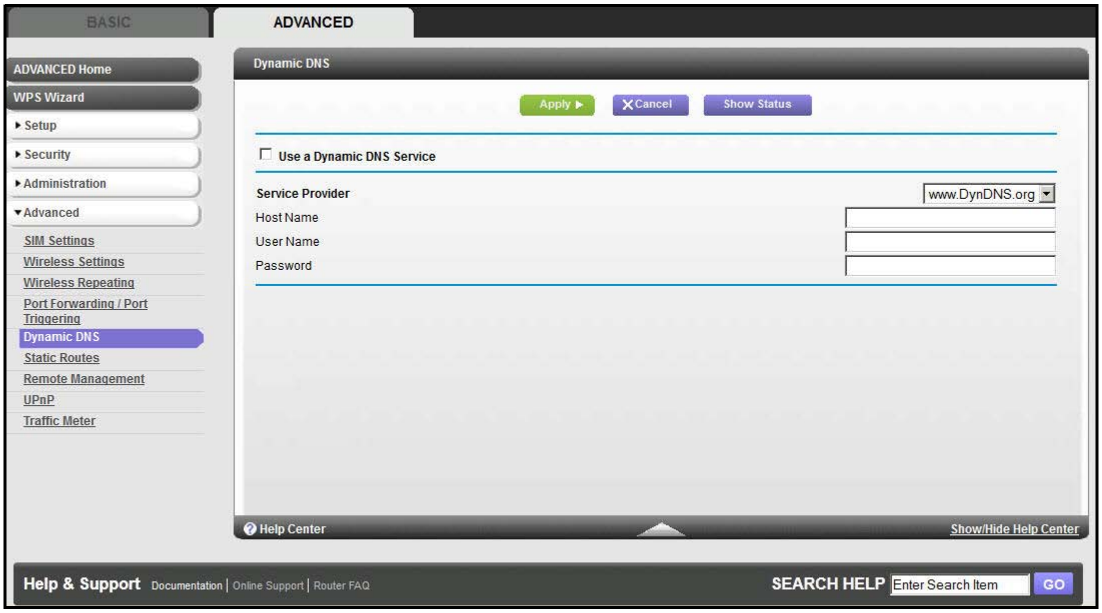
Dynamic DNS

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

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

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

On the **ADVANCED** tab, select **Advanced > Dynamic DNS** to display the following screen:



Dynamic DNS

□ Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name

User Name

Password

➢ **To set up Dynamic DNS:**

1. Register for an account with one of the Dynamic DNS service providers whose URLs appear in the Service Provider list.
2. Select the **Use a Dynamic DNS Service** check box.
3. Select the URL of your Dynamic DNS service provider. For example, for DynDNS.org, select **www.dyndns.org**.
4. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
5. Type the user name for your Dynamic DNS account. This name is the name that you use to log in to your account, not your host name.
6. Type the password (or key) for your Dynamic DNS account.
7. Click **Apply** to save your configuration.

Static Routes

Static routes provide more routing information to your router. Under usual circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure more static routes. You 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.

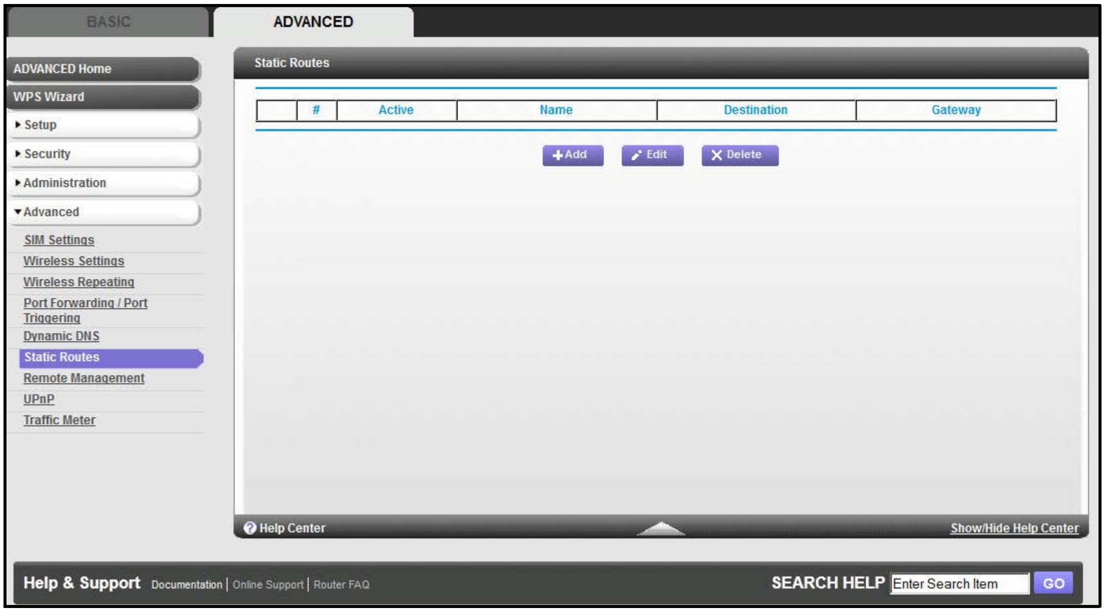
When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0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

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 since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

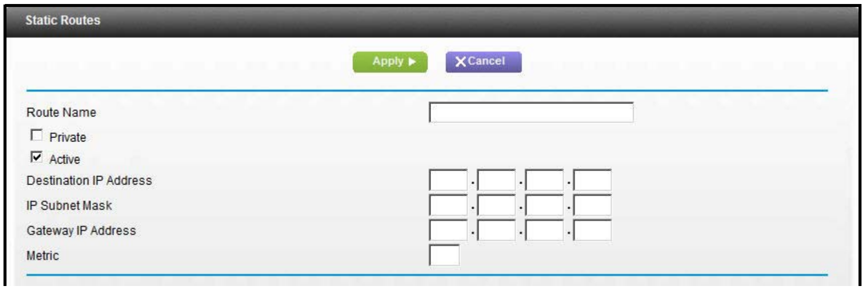
➢ To set up a static route:

1. Select **ADVANCED > Advanced > Static Routes** to display the following screen:



	#	Active	Name	Destination	Gateway

2. Click **Add** to display the following screen:



Route Name

□ Private

☑ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

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 a router 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 connection is a direct connection, set it to 1.

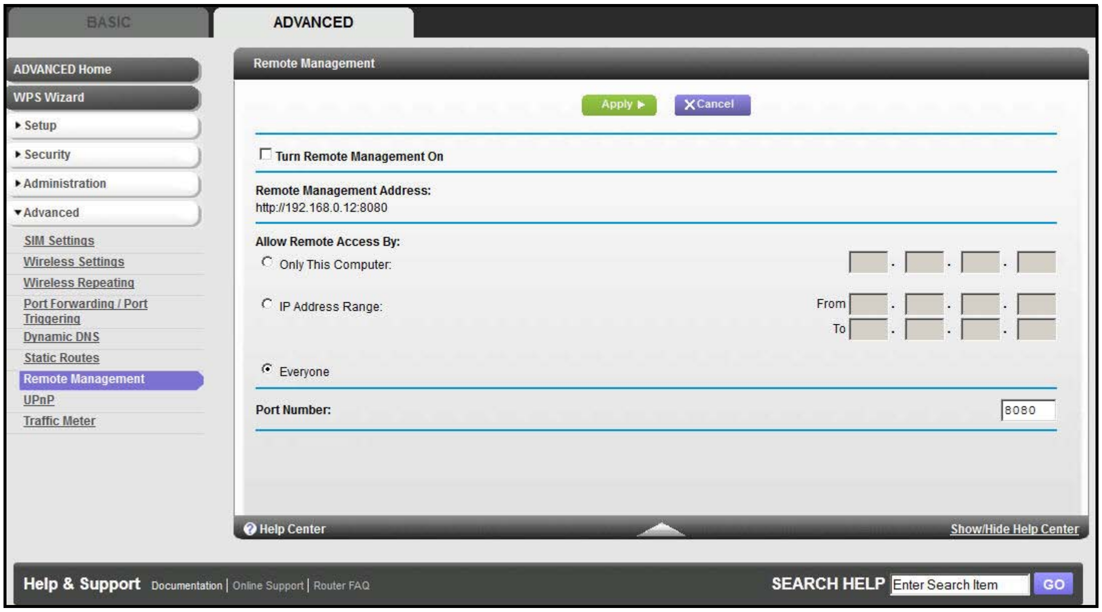
10. Click **Apply** to add the static route.

Remote Management

The remote management feature lets you upgrade or check the status of your router over the Internet.

➢ To set up remote management:

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



Remote Management

□ Turn Remote Management On

Remote Management Address:
http://192.168.0.12:8080

Allow Remote Access By:

○ Only This Computer: ___ . ___ . ___ . ___

○ IP Address Range: From ___ . ___ . ___ . ___ To ___ . ___ . ___ . ___

● Everyone

Port Number: 8080

> **Note:** *Be sure to change the router’s default login password to a secure password. The ideal password should contain no dictionary words from any language and contain uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.*

2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, select the extent of external IP addresses that are allowed access to 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 is 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 to define the allowed range.
- 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 through 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 **Apply** to have your changes take effect.
6. When accessing 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.

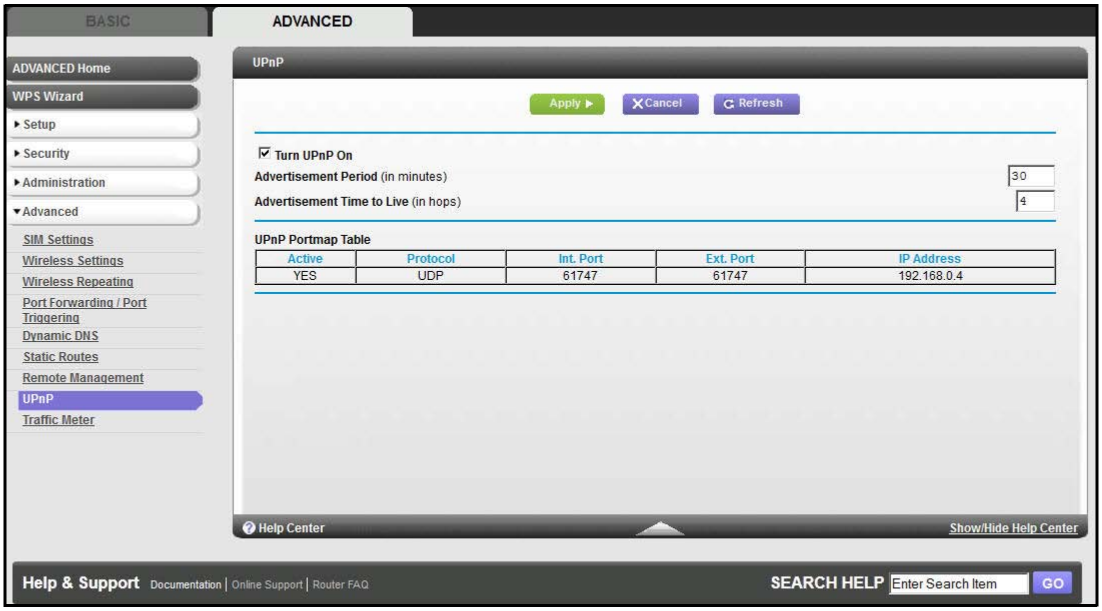
Universal Plug and Play

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

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

➢ To turn on Universal Plug and Play:

1. Select **ADVANCED > Advanced > UPnP**. The UPnP screen displays.



☑ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time to Live (in hops) 4

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
YES	UDP	61747	61747	192.168.0.4

2. The available settings and information in this screen are:

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

Advertisement Period. The advertisement period is 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.

Advertisement Time to Live. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. 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.

UPnP Portmap Table. 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.

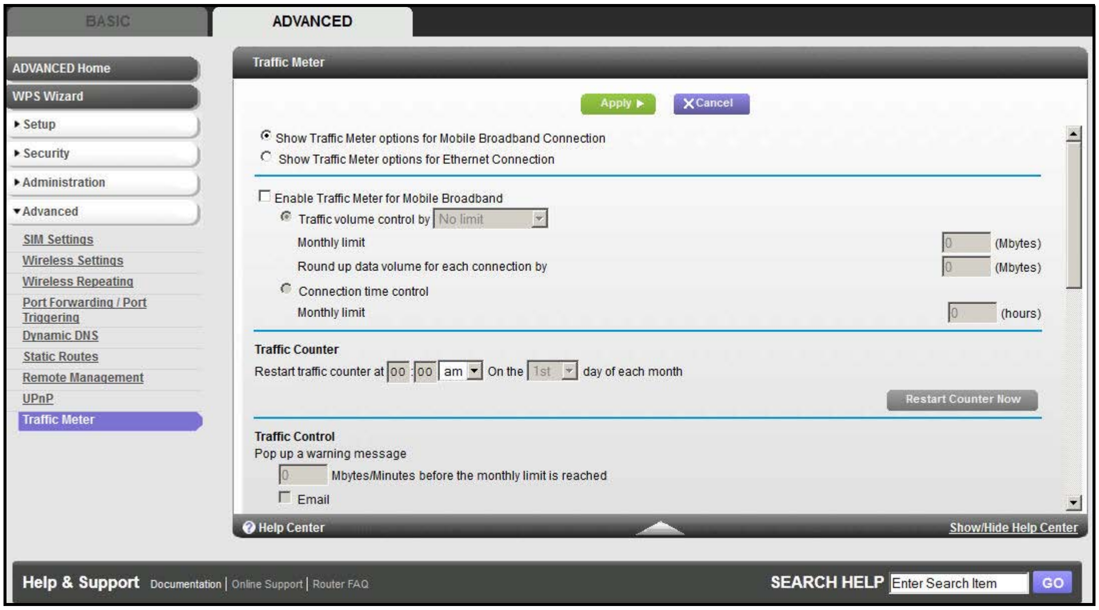
3. Click **Apply** to save your settings.

Traffic Meter

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

➢ **To monitor Internet traffic:**

1. Click **ADVANCED > Advanced > Traffic Meter** to display the following screen:



Traffic Meter

● Show Traffic Meter options for Mobile Broadband Connection
○ Show Traffic Meter options for Ethernet Connection

□ Enable Traffic Meter for Mobile Broadband
● Traffic volume control by No limit
Monthly limit 0 (Mbytes)
Round up data volume for each connection by 0 (Mbytes)
○ Connection time control
Monthly limit 0 (hours)

Traffic Counter
Restart traffic counter at 00 : 00 am On the 1st day of each month

Traffic Control
Pop up a warning message
0 Mbytes/Minutes before the monthly limit is reached
□ Email

2. To enable the traffic meter, select the **Enable Traffic Meter for Internet** check box.

3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:

   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.

4. You can limit the amount of data traffic allowed per month by specifying how many Mbytes per month are allowed or by specifying how many hours of traffic are allowed.
5. Set the traffic counter to begin at a specific time and date.
6. Set up traffic control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   - The Internet LED blinks green or amber.
   - The Internet connection is disconnected and disabled.
7. Set up Internet traffic statistics to monitor the data traffic.
8. Click the **Traffic Status** button to get a live update of the status of Internet traffic on your router.
9. Click **Apply** to save your settings.

8. Troubleshooting

8

This chapter gives information about troubleshooting your router. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?

  Go to *Basic Functioning* on page 85.

- Have I connected the router correctly?

  Go to *Basic Functioning* on page 85.

- I cannot access the router’s configuration with my browser.

  Go to *Troubleshoot Access to the Router Main Menu* on page 87.

- I have configured the router but I cannot access the Internet.

  Go to *Troubleshoot the ISP Connection* on page 88.

- I have configured the router but I cannot access my local network.

  Go to *Troubleshoot a TCP/IP Network Using the Ping Utility* on page 89.

- How do I set daylight saving time?

  Go to *Problems with Date and Time* on page 91.

- I want to clear the configuration and start over again.

  Go to *Restore the Default Configuration and Password* on page 91.

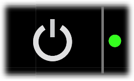
Basic Functioning

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 LED is lit.
2. After approximately a minute, verify the following:
   - **a.** The Power LED is still solid green. An amber light indicates that the unit has failed its power-on self-test (POST).
   - **b.** The Internet LED is lit.
   - **c.** The WiFi LED is lit. The WiFi radio is on by default.
   - **d.** The LAN LED is lit when any local ports are connected.

     If a LAN port LED on the back of the unit is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED is amber.
   - **e.** The WAN LED is lit when the router is connected to a wired modem.
   - **f.** The Signal Quality LED is lit when the router has detected a mobile broadband signal.

If any of these conditions does not occur, refer to the following table.

LED		Action
Power 	Power LED is off.	• Make sure that the power cord is correctly connected to your router, and that the power supply adapter is correctly connected to a functioning power outlet. • Check that you are using the power adapter supplied by NETGEAR for this product. If the error persists, you might have a hardware problem and should contact technical support.
	Power LED is amber.	A fault exists within the router. Try to clear the fault as follows: • Cycle the power to see if the router recovers. • Clear the router's configuration to factory defaults. This action sets the router's IP address to www.routerlogin.net. This procedure is explained in *Restore the Default Configuration and Password* on page 91. If the error persists, you might have a hardware problem and should contact technical support.

LED		Action
Internet	Internet LED is off.	Be sure the SIM card that you received is in the router. SIM cards from other devices do not function in the router, and this SIM card does not function in other devices.
	Internet LED is amber.	The router cannot connect to the Internet. Check the Internet connection option being used. • For the mobile broadband connection option, check the Signal Quality LEDs. • For the Ethernet connection option, check the WAN Port LED.
	Internet LED is blinking amber and green.	The traffic meter feature is enabled, and the limit set has been reached.
WiFi	WiFi LED is off.	The WiFi radio has been turned off. If you want a WiFi connection with the router, press the **WiFi** button to turn the WiFi radio back on.
	WiFi LED is not blinking.	If this LED does not blink when you are attempting to send data over the WiFi link, log in to the router menu using the Ethernet LAN connection, and check your router’s wireless (WiFi) configuration.
LAN	LAN LED is off.	If this LED does not light when an Ethernet connection is made, check the following: • Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation. • Make sure that power is turned on to the connected hub or workstation.
WAN	WAN LED is off.	If this LED does not light when an Ethernet connection is made using the Ethernet connection option, check the following: • Make sure that the Ethernet cable connections are secure at the router and at the modem. • Make sure that power is turned on to the modem.
Signal Quality	Signal Quality LED is off.	If this LED does not light when the mobile broadband connection option is used, check the following: • Check with your ISP to ensure that good coverage exists in the area. • Ensure that your mobile broadband account is active. • Ensure that the SIM card is inserted correctly into the router. • Locate the router near the window or other area of the building. Make sure that the Signal Quality LED is lit, indicating that mobile broadband coverage exists with the router. • Log in to the router menu and check the Internet configuration. Check that the user name, password, and APN with ISP are set correctly. If you use a PIN to connect to the Internet, make sure that it is entered correctly.

Troubleshoot Access to the Router Main Menu

If you are unable to access the router main menu 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 as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254.

Note: If your computer's IP address is shown as 169.254.x.x:
Recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This action sets the router's IP address to www.routerlogin.net. This procedure is explained in *Restore the Default Configuration and Password* on page 91.
- 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 factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

If the router does not save changes you have made in the web management interface, check the following:

- When entering configuration settings, be sure to 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 web browser might be caching the old configuration.

Troubleshoot the ISP Connection

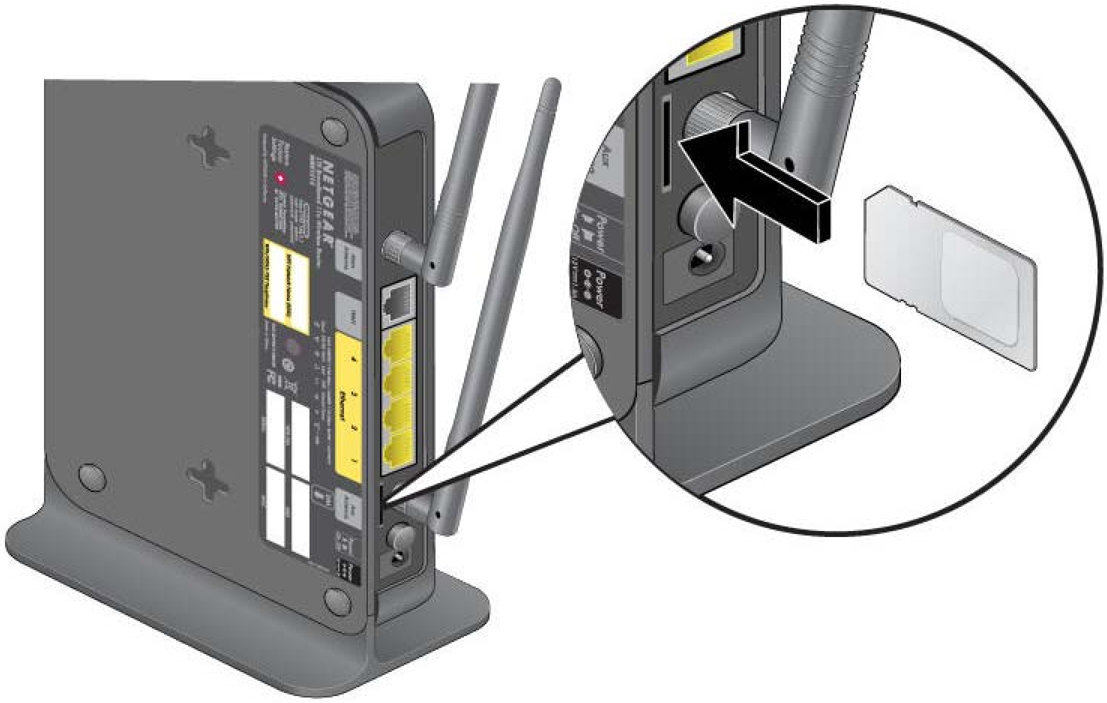
Check these possible sources of trouble if you are having difficulty connecting to or browsing the Internet.

Connect to the Internet

If unable to connect to Internet, check the following:

1. The Internet account is active.

   If your ISP has provided you with a SIM card and you have not inserted it into the SIM card slot on the back of the router yet, do so now.



2. Wireless broadband coverage is available where the unit is located.
3. Access the router main menu to verify that the broadband settings are correct. Check with your ISP if you are unsure.
4. Check the location of the router.

   a. Move the router closer to a window for better access to the Internet signal. A Signal Quality LED that is off indicates no coverage.

   b. Maintain recommended minimum distances between NETGEAR equipment and household appliances to reduce interference.

Troubleshoot Internet Browsing

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet:

- The traffic meter is enabled, and the limit might have been reached.

  By configuring the traffic meter not to block, you can resume Internet access. If you have a usage limit, your ISP might charge you for the overage.

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation*.*

- Your computer might not have the router configured as its TCP/IP router.

  If your computer obtains its information from the router by DHCP, reboot the computer, and verify the router address.

Troubleshoot a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal 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 TCP/IP network by using the ping utility in your computer.

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 PC running Windows 95 or later:**

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

   ```
   ping 192.168.0.1
   ```
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 working correctly, you could have one of the following problems:

- Wrong physical connections
  - Make sure that the LAN LED is on. If the LED is off, follow the instructions in *Connect to the Internet* on page 88.
  - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
  - Verify that the IP address for your router and your workstation 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.

➢ **To test the path:**

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 as in the previous section are displayed. When you do not receive replies:

- Check that your computer has the IP address of your router listed as the default router. If the IP configuration of your computer gets assigned by DHCP, this information is not visible in your computer’s Network Control Panel. Verify that the IP address of the router is listed as the default router.
- Make sure that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- 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 Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing only traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If so, you need to configure your router to clone or spoof the MAC address from the authorized computer.

Problems with Date and Time

The Email screen displays the current date and time of day. The router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000.
  Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have completed configuring the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour.
  Cause: The router does not automatically sense daylight saving time. On the Schedule screen, select an appropriate time zone and set or clear the **Automatically adjust for Daylight Savings Time** check box.

Restore the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's admin password to **password** and the IP address to **www.routerlogin.net**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase feature (see *Erase* on page 55).
- Press the **Restore Factory Settings** button on the bottom of the router for 6 seconds. Use this method for cases when the administration password or IP address is not known.

The factory default settings are shown in *Factory Default Settings* on page 93.

Supplemental Information

A

This appendix provides the following information:

- *Factory Default Settings*
- *Technical Specifications*

Factory Default Settings

Use the Restore Factory Settings button on the bottom of your router to reset all settings to their original factory default settings. This action is called a hard reset. To perform a hard reset, press and hold the **Restore Factory Settings** button for 6 seconds. Your router returns to the factory configuration settings that are shown in the following table.

Feature		Default Behavior
Router login	User login URL	http://192.168.0.1
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1500
	Port speed	AutoSense
Local network (LAN)	LAN IP	www.routerlogin.net
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Disabled
Firewall	Inbound communication from the Internet	Disabled (except traffic on port 80, the HTTP port)
	Outbound communication to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Broadband settings	Internet connection mode	Always use Mobile Broadband Connection
Mobile broadband	Internet service provider	Verizon
	APN	vzwinternet
	Access Number	*99***3#
	PDP type	IPV4V6
	User name	None required

Feature (continued)		Default Behavior (continued)
WiFi	Wireless communication	Enabled
	SSID name	See label on the bottom of router
	Security	WPA-PSK/WPA2-PSK mixed mode
	Broadcast SSID	Enabled
	Transmission speed	Auto (Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.)
	Country/region	United States
	RF channel	Auto
	Operating mode	Up to 145 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open system
	Wireless Card Access List	All wireless stations allowed

Technical Specifications

Technical Specifications	
Network protocol and standards compatibility	TCP/IP, DHCP
Power adapter	• North America: 120V AC, 60 Hz, input • 12V DC @ 1.5A output
Physical specifications	• Dimensions: 6.8 in. x 5.03 in. x 1.28 in. (173 mm x 128 mm x 33 mm) • Weight: 0.65 lbs without the stand (0.29 kg)
Environmental specifications	• Operating temperature: 0° to 40°C (32º to 104ºF) • Operating humidity: 90% maximum relative humidity, noncondensing
Interface specifications	• LAN: 10BASE-T or 100BASE-Tx, RJ-45 • WAN: 10BASE-T or 100BASE-TX, RJ-45
Antenna connection (optional)	• SMA connector

Wall-Mounting

B

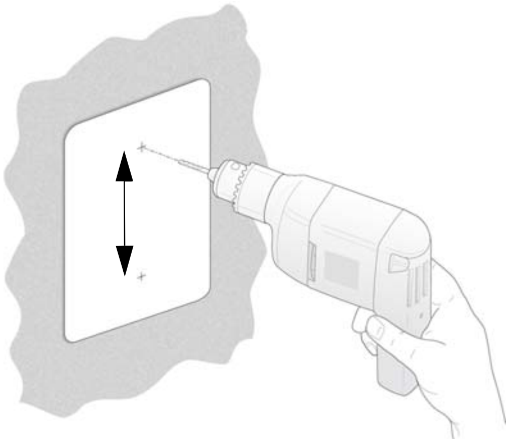
This appendix provides instructions for wall-mounting your router.

Your router’s location can affect wireless connections. For example, the thickness and number of walls the wireless signal needs to pass through might limit its range. For best results, place your router:

- Near an AC power outlet, close to computers you plan to connect with Ethernet cables, and near locations where you use wireless computers. For best signal strength, the router should be within line of sight of your wireless devices.
- In an elevated location, keeping the number of walls and ceilings between the router and your wireless computers to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, or the base for a cordless phone.

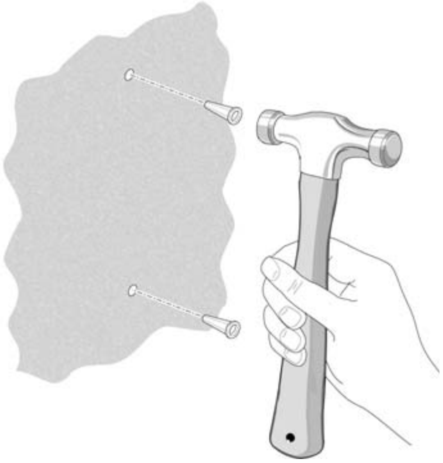
➢ **To wall-mount the router:**

1. Drill holes in the wall where you want to wall-mount the router.



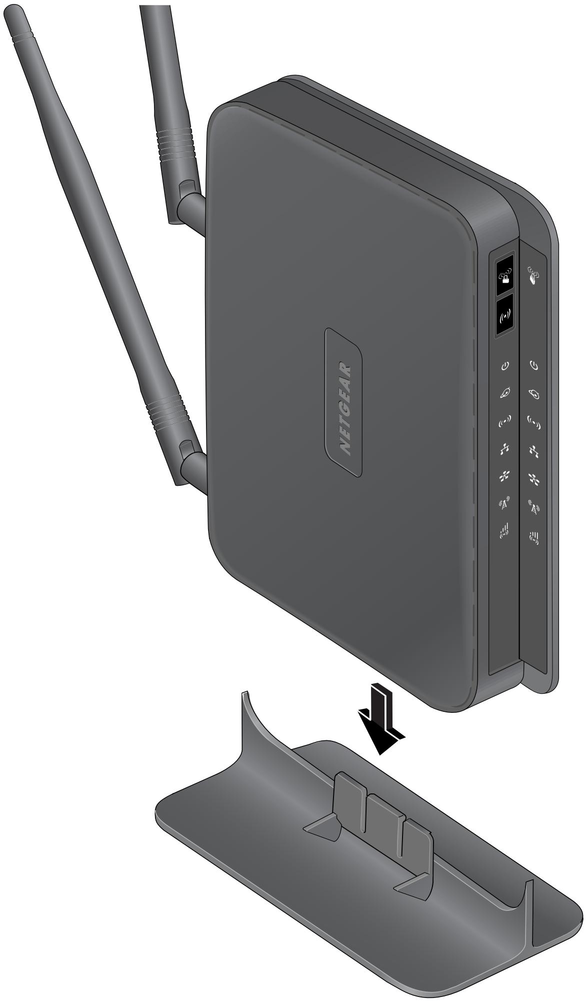
Holes should be 9.5 in. (24.1 cm) center to center.

2. Install wall anchors in the holes.

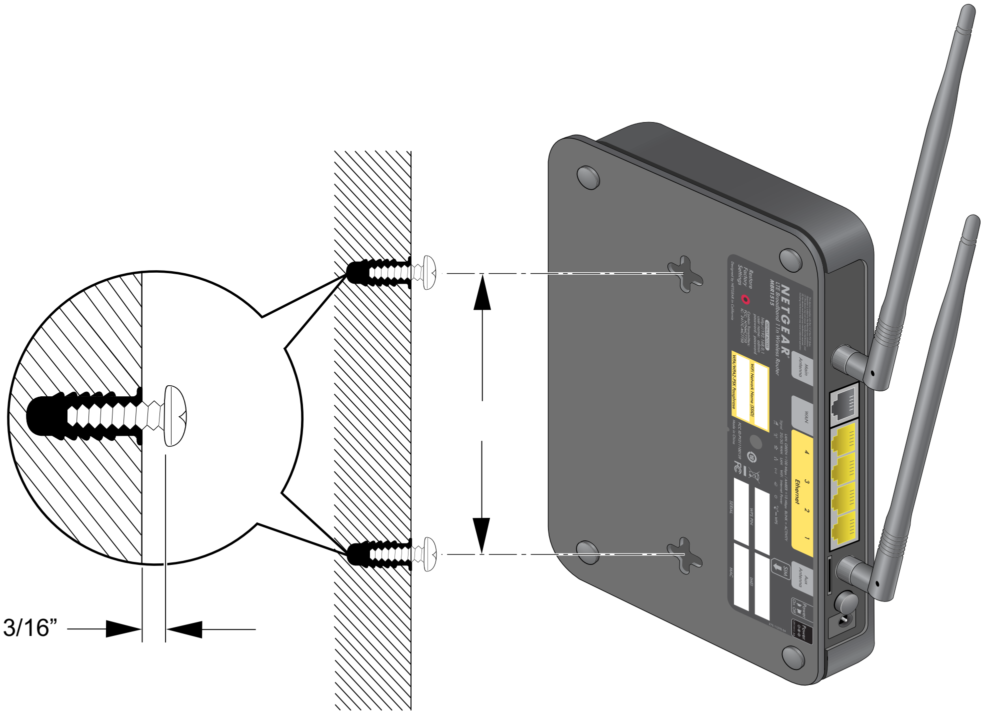


Use pan head Phillips wood screws, 3.5 x 20 mm (diameter x length, European) or No. 6 type screw, 1 inch long (U.S.).

3. Detach the stand from the unit.



4. Insert screws into the wall anchors, leaving 3/16 inch (0.5 cm) of each screw exposed.



5. For best wireless performance, position the antennas at right angles to each other.

Notification of Compliance

C

NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

Note: 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.

Note: 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.

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.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the LTE Broadband 11n Wireless Router MBR1515 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 market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Interference Reduction Table

The table below 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

Index