NETGEAR®

N300 Wireless Router JWNR2000v3

User Manual

May 2013
202-11281-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

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

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

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

Trademarks

Contents

Chapter 5 Security

Chapter 6 Administration

Chapter 7 Advanced Settings

Hardware Setup

1

Getting to know your router

This manual provides you with an easy and secure way to set up a wireless home network.

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

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. The next chapter explains how to set up your Internet connection.

This chapter contains the following sections:

Unpack Your Router

Your box contains the following items:

- N300 Wireless Router JWNR2000v3
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Installation guide with cabling and router setup instructions

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

Hardware Features

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

Label

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

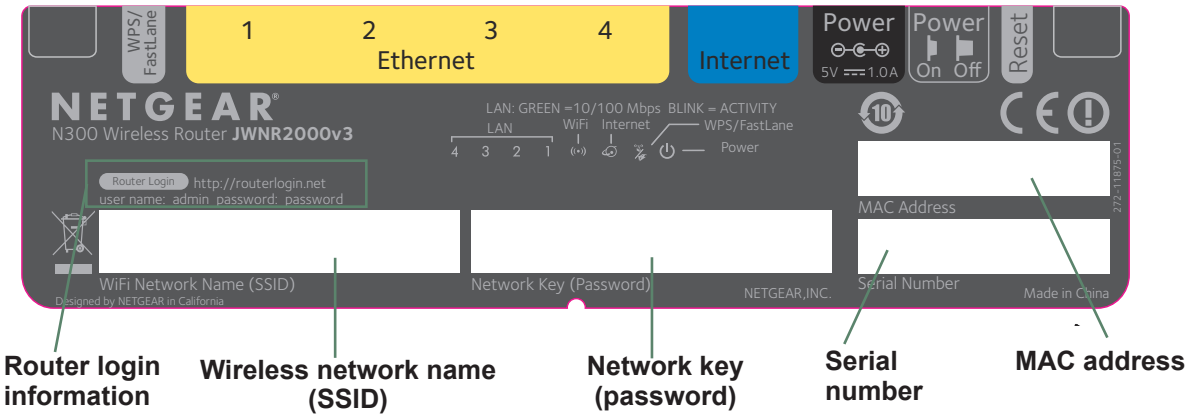


Figure 1. Label on router bottom

Front Panel

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

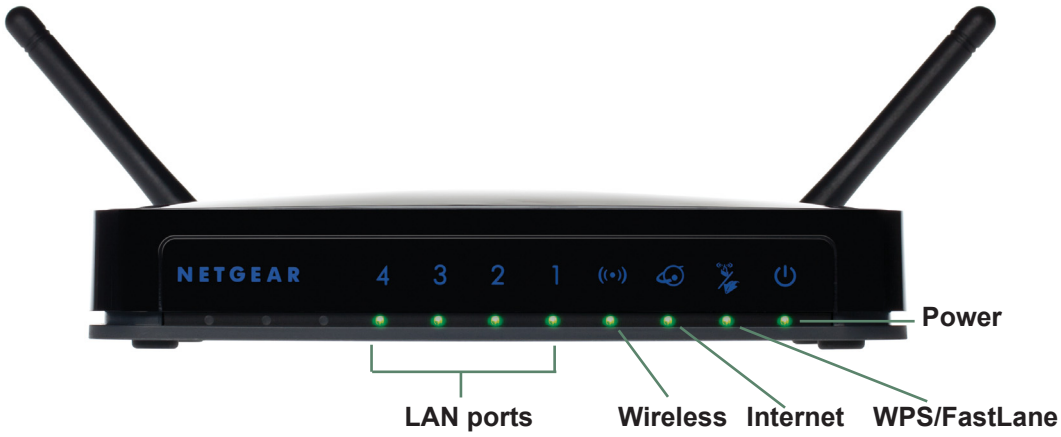


Figure 2. Front panel LEDs and icons

Table 1. Front panel LEDs

Icon	LED Activity	Description
LAN ports 1–4 	Solid green Blinking green Off	The local port is connected to a 10/100 Mbps device. Data is being transmitted at 10/100 Mbps. No link is detected on this port.
Wireless 	Solid green Blinking green Off	The wireless interface is enabled. Data is being communicated over the wireless network. The wireless interface is turned off.
Internet (WAN) 	Solid green Blinking green Off	The router has acquired an Internet address. Data is being communicated with the Internet. No Ethernet cable is connected to the modem.
WPS/FastLane 	Solid green Blinking green Off Solid green Off	WPS mode: • WPS mode is enabled. • WPS mode is available for connection. • WPS mode is disabled. FastLane mode: • FastLane mode is enabled. • FastLane mode is disabled.
Power 	Solid green Off	Power is supplied to the router. Power is not being supplied to the router.

Back Panel

The back panel has the following features:

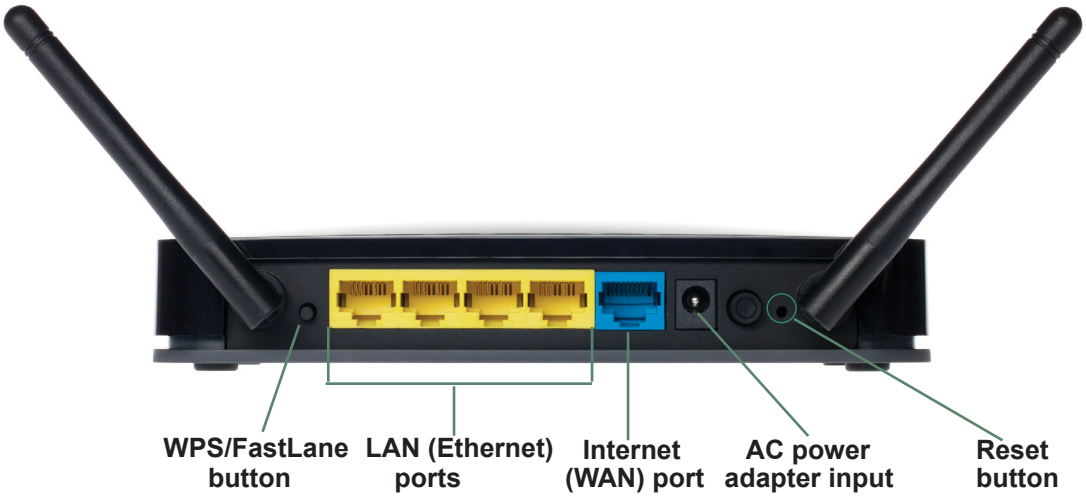


Figure 3. Back panel

Position Your Router

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

- Near the center of the area where your computers and other devices operate and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, 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.
- With the antennas in a vertical position to provide the best side-to-side coverage or in a horizontal position to provide the best up-and-down coverage, as applicable.

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).

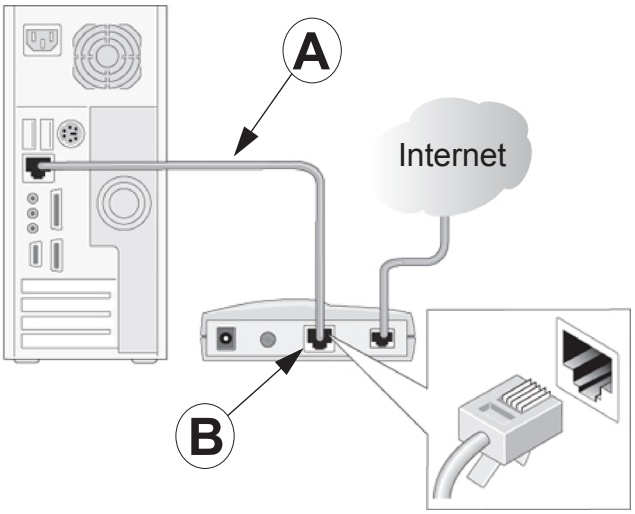
Cable Your Router

The installation guide that came in the box includes a cabling diagram. This section walks you through cabling with detailed illustrations.

➢ **To connect the router, the computer, and the modem:**

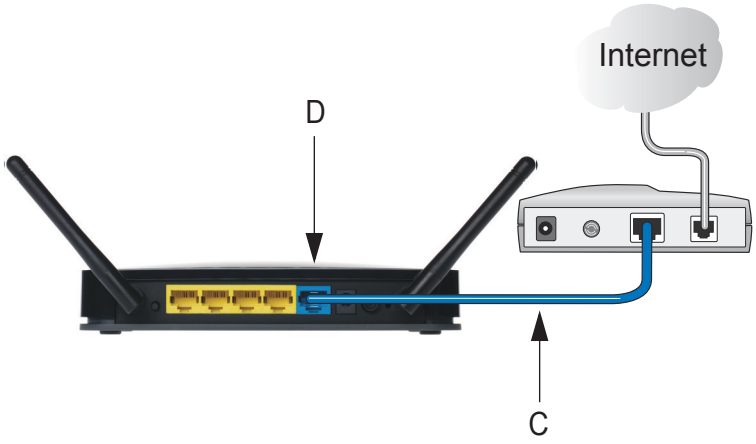
1. Unplug and turn off the broadband modem.
2. Locate the cable (A) that connects your computer to the modem.

Disconnect the cable at the modem end only (B). You will connect it to the router later.



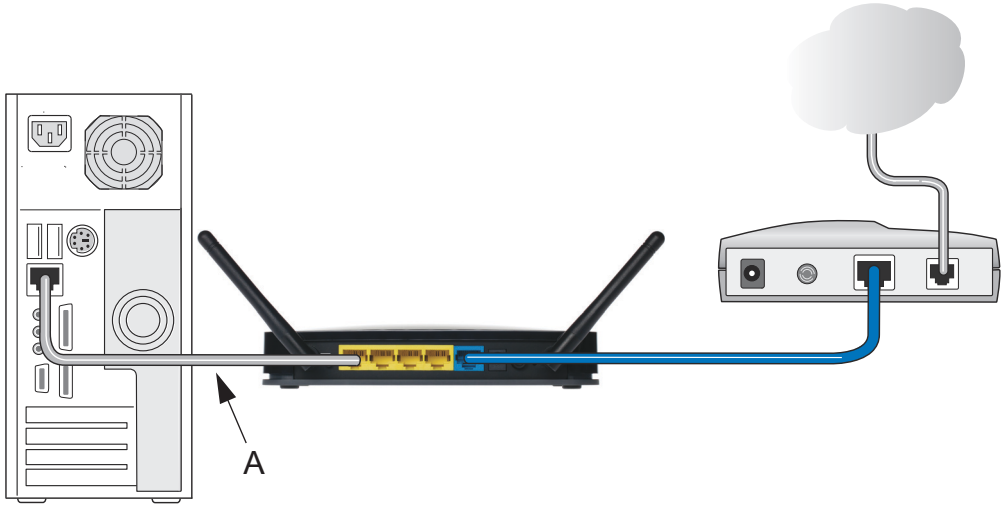
3. Connect the blue Ethernet cable (C) that came with the router to the Internet (WAN) port (D) on the router, and to the Ethernet port on your broadband modem.

   The Ethernet cable and the Internet port label are color coded.



4. Locate the cable (A) that is still attached to your computer.

   Insert that cable into a yellow LAN port on the router, as shown in the following figure:



5. Connect any additional wired computers to your router by inserting an Ethernet cable from a computer into one of the three remaining LAN ports.
6. Start your network in the correct sequence.

   See the following procedure.

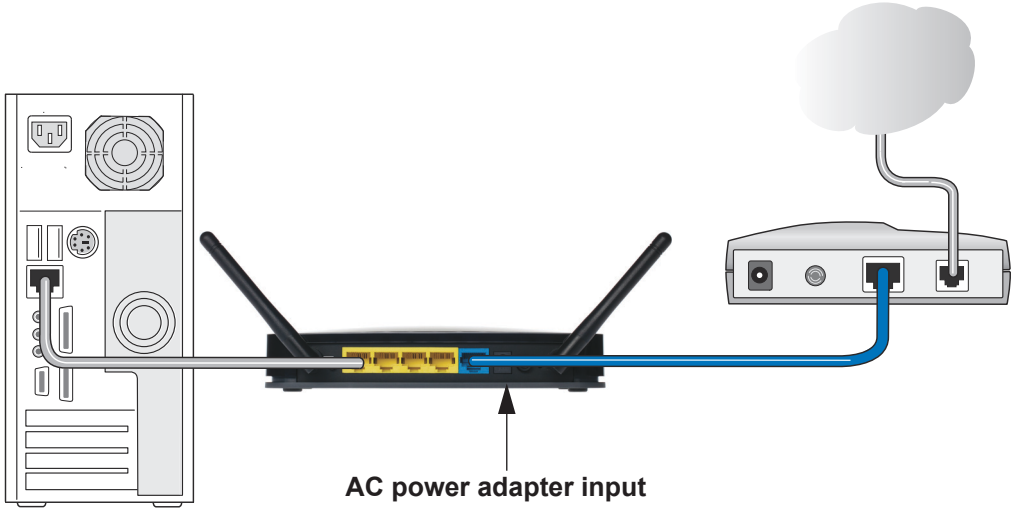
CAUTION:

Failure to start or restart your network in the correct sequence could prevent you from accessing the Internet.

➢ **To start your network:**

1. Plug in and turn on the cable or DSL modem. Wait two minutes.
2. Plug the power adapter into the AC power adapter input on the router.

3. Plug the other end of the power adapter into a power outlet. Wait two minutes.



It might take several minutes for your router to establish a connection with your computer and your Internet provider.

After correctly cabling your router, see *NETGEAR genie Setup* on page 16 for information about how to set up your network.

2. Access the Router

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.

This chapter contains the following sections:

Router Setup Preparation

You can set up your router with the NETGEAR genie automatically, or you can use the genie menus and screens to set up your router manually. Before you start the setup process, get your ISP information and make sure the computers and devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

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

Gather ISP Information

If you have DSL broadband service, you might need the following information to set up your router and to check that your Internet configuration is correct:

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

When your Internet service starts, your Internet service provider (ISP) typically gives you all the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your router automatically logs you in.

Wireless Devices and Security Settings

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

Types of Logins

Different types of logins have different purposes:

- **Router login**. Logs you in to the router interface from NETGEAR genie. For more information for details about this login, see *Use NETGEAR genie after Installation* on page 17.
- **ISP login**. Logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network key or password**. Your router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label on the bottom of your router.

It is important that you understand the differences between the login types so that you know which login to use when.

NETGEAR genie Setup

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

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

1. Turn on the router, 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.
   - The first time that you set up the Internet connection for your router, the browser goes to http://www.routerlogin.net, and the NETGEAR genie screen displays.
   - If you already used the NETGEAR genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR genie screen. See *Use NETGEAR genie after Installation* on page 17.
4. Follow the onscreen instructions to complete NETGEAR genie setup.

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

   If the browser cannot display the web page, try these troubleshooting tips:

   - Make sure that the computer is connected to one of the four LAN Ethernet ports, or wirelessly to the router.
   - Make sure that the router has full power, and that its Wireless LED is lit.
   - Close and reopen the browser to make sure that the browser does not cache the previous page.
   - Browse to **http://www.routerlogin.net**.

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

➢ **To troubleshoot Internet access problems:**

If the router does not connect to the Internet, follow these troubleshooting steps:

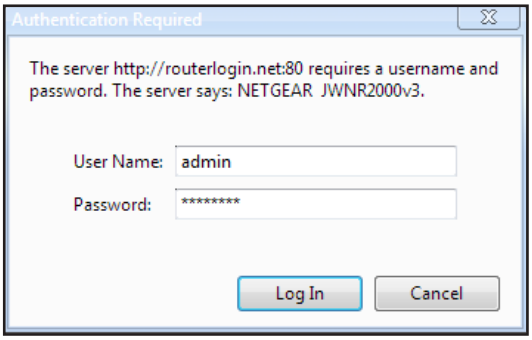
1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 8, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR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

Use NETGEAR genie after Installation

When you first set up your router, NETGEAR genie automatically starts when you launch an Internet browser on a computer that is connected to the router. You can use NETGEAR genie again 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://www.routerlogin.net** or **http://www.routerlogin.com**.

   The login window displays:



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. For more information, see Types of Logins on page 16.*

Upgrade Router Firmware

When you set up your router and are connected to the Internet, the router automatically checks to see if newer firmware is available. If it is, a message displays on the top of the screen. For more information about upgrading firmware, see *Upgrade the Router Firmware* on page 70.

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

CAUTION:

Do not try to go online, turn off the router, shut down the computer, or do anything else to the router until the router finishes restarting. Wait until the progress bar on the NETGEAR genie screen completes.

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 five sections of the dashboard to view more detailed information. The left column has the menus, and an ADVANCED tab is at the top. Use the ADVANCED tab to access additional menus and screens.

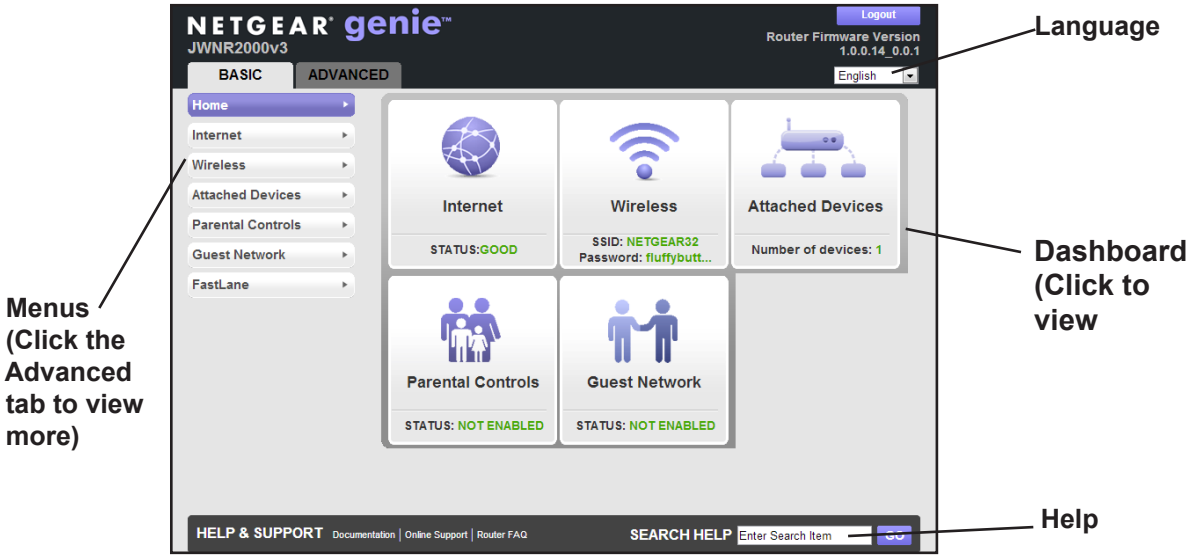


Figure 4. BASIC Home Screen

The dashboard contains these components:

- **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.
- **Guest Network**. Set up a guest network to allow visitors to use your router's Internet connection.
- **FastLane**. Enable FastLane mode to reserve bandwidth on the router for a trusted IP address that you specify.
- **Basic tab. Configure the basic settings of your router using the menus available from this tab.**
- **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 to get information, help, and product documentation. These links work once you have an Internet connection.
- **Language menu**. Select your preferred language from the drop-down menu at the top right corner of the screen.

Join Your Wireless Network

Choose either the manual or the WPS method to join your wireless network. For instructions for how to set up a guest network, see *Set Up a Guest Network* on page 35.

WPS Method

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

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

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

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

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

Manual Method

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

➢ **To connect manually:**

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

   This software scans for all wireless networks in your area.

2. Look for your network and select it.

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

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

NETGEAR genie App and genie Mobile App

The genie app is the easy dashboard for managing, monitoring, and repairing your home network. It allows you to automatically repair common wireless network problems. It also provides easy access to router features like Live Parental Controls, guest access, broadband usage meter, speed test, and more.

For more information, see the *NETGEAR genie Apps User Manual*.

Figure 5. genie app dashboard

You can use the genie mobile app on your iPhone, iPad, or Android phone.

Figure 6. genie mobile app home screen

NETGEAR genie Basic Settings

3

Your Internet connection and network

This chapter contains the following sections:

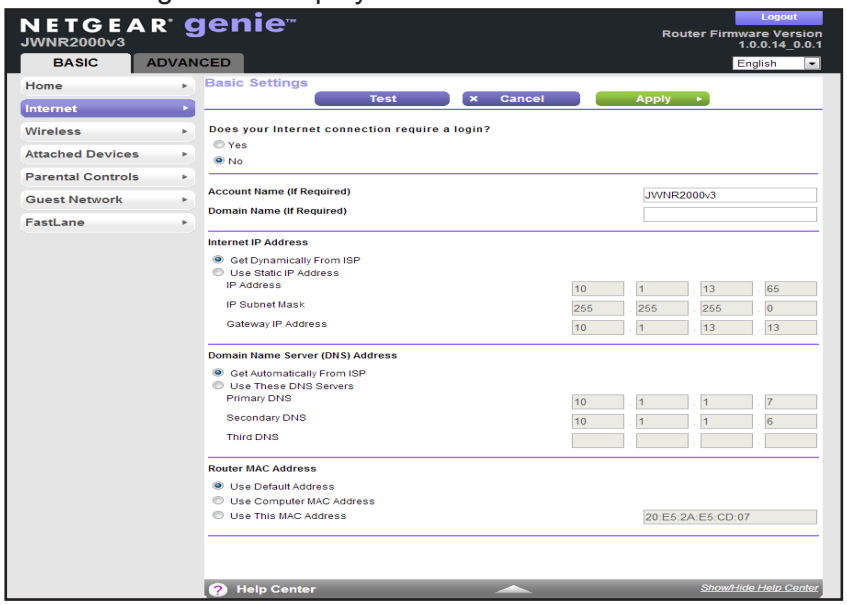
Basic Settings

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

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

1. From the BASIC Home screen, select **Internet**.

   The following screen displays:



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

2. Select a radio button in the **Does Your Internet Connection Require a Login?** field as follows:
   - **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.
3. 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.

4. Click **Apply**.

   You settings are saved.

5. Click **Test** to test your Internet connection.

   If the NETGEAR website does not display within 1 minute, see *Chapter 8, Troubleshooting*.

Basic Settings Screen Fields

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

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

If your ISP does not require a login and you selected no, the following screen displays:

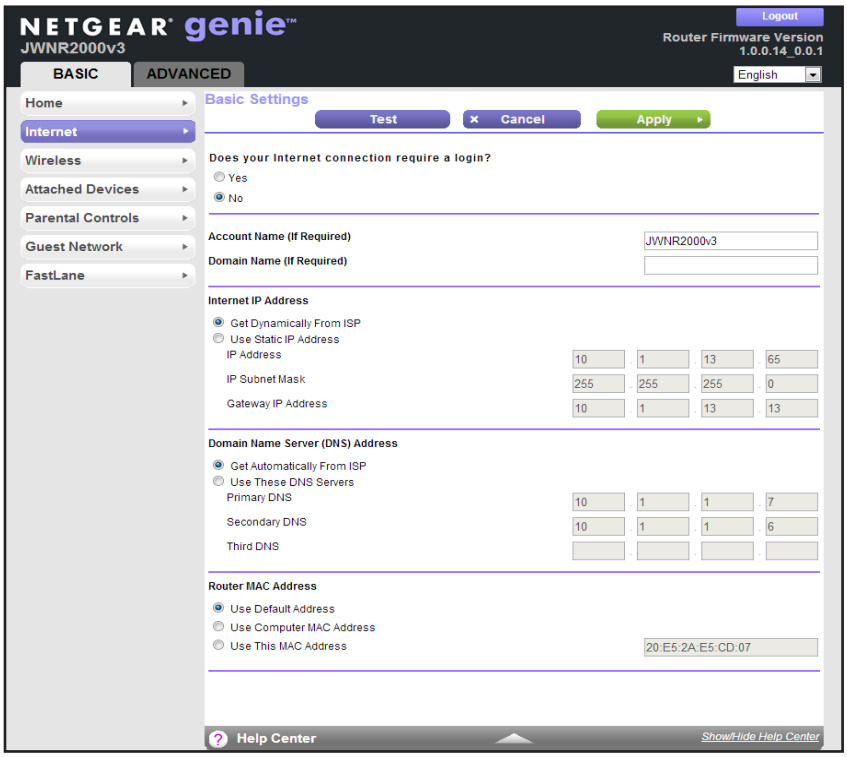


Figure 7. Basic Settings Screen When ISP Does Not Require Login

The following fields display when no login is required:

- **Account Name (If required)**. Enter the account name that your ISP provided. It might also be called the host name.
- **Domain Name (If required)**. Enter the domain name that your ISP provided.
- **Internet IP Address**. Select one of these options:
  - **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
  - **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's router to which your router will connect.
- **Domain Name Server (DNS) Address**. The DNS server is used to look up site addresses based on their names.
  - **Get Automatically From ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.

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

- **Router MAC Address**. The Ethernet MAC address that the router uses on its Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your router to use your computer's MAC address (this feature is also called cloning). Select one of these options:
  - **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 must use the one computer that is allowed by the ISP.
  - **Use This MAC Address**. Enter the MAC address that you want to use.

If your ISP requires a login and you selected Yes, the following screen displays:

Figure 8. Basic Settings Screen When ISP Requires a Login

The following fields display when your ISP requires a login:

- **Internet Service Provider Encapsulation**. ISP types. The choices are PPPoE, PPTP, or L2TP.
- **Login**. The login name provided by your ISP. It is often an email address.
- **Password**. The password that you use to log in to your ISP.

- **Service Name (If Required)**. If your ISP provided a service name, enter it here.
- **Connection Mode**. Always On, Dial on Demand, or Manually Connect.
- **Idle Timeout (In minutes)**. If you want to change the login time-out, enter a new value in minutes. This setting determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.
- **Internet IP Address**. Select one of these options:
  - **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
  - **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's router to which your router will connect.
- **Domain Name Server (DNS) Address**. The DNS server is used to look up site addresses based on their names.
  - **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
  - **Use These DNS Servers**. If you know that your ISP requires specific servers, select this option. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
- **Router MAC Address**. The Ethernet MAC address that the router uses on its Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your router to use your computer's MAC address (this feature is also called cloning). Select one of these options:
  - **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 must use the one computer that is allowed by the ISP.
  - **Use This MAC Address**. Enter the MAC address that you want to use.

Basic Wireless Settings

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

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

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

If you change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

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

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

1. From the BASIC Home screen, select **Wireless**.

   The following screen displays:

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

2. Make any changes that are needed.
3. Click **Apply**.

   Your settings are saved.

4. Set up and test your wireless devices and computers to make sure that they can connect wirelessly.

   If they do not, check the following:

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

Wireless Settings Screen Fields

You can configure the following wireless settings:

- **Region**. The location where the router is used. Select from the countries in the drop-down menu. In the United States, the region is fixed to United States and is not changeable.
- **Enable SSID Broadcast**. This setting 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**.
- **Enable Wireless Isolation**. If this check box is selected, wireless computers or devices that join the network can use the Internet but cannot access each other or access Ethernet devices on the network.
- **Name (SSID)**. The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and ***NETGEAR strongly recommends that you do not change this setting.***
- **Channel**. This setting is the wireless channel the gateway uses. 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). If you experience interference, experiment with different channels to see which is the best.
- **Mode**:
  - **Up to 54 Mbps**. This legacy mode uses a maximum speed of Mbps for b/g networks.
  - **Up to 150 Mbps**. (Default) This neighbor-friendly mode does not interfere with neighboring wireless networks.
  - **Up to 300 Mbps**. Performance mode uses the maximum wireless-N speed of up to 300 Mbps.
- **Security Options**. The Security Options section of the Wireless Settings screen lets you change the security option and password. **Do not disable security**. For more information about the security options, see *Security Options* on page 28.

Note: WEP is a legacy security setting. NETGEAR recommends that you use WPA2 or WPA security unless you have legacy wireless equipment that supports only WEP. WEP encryption is available only when the Mode setting is Up to 54 Mbps.

Security Options

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

receive authorization to connect to your network. Wi-Fi Protected Access (WPA) has several options including pre-shared key (PSK) encryption.

This section presents an overview of the security options and provides guidance on when to use which option.

WEP Encryption

WEP uses an old encryption method and can be easily decoded with today's powerful computers. Use this mode only when you have a very old legacy wireless client that does not support WPA-PSK. The Wi-Fi Alliance highly recommends against using WEP and plans to make it obsolete. If you do decide to use WEP, see *Change the WEP Security Option* on page 29 for the procedure.

WPA Encryption

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

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

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

WPS-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security.

Change the WEP Security Option

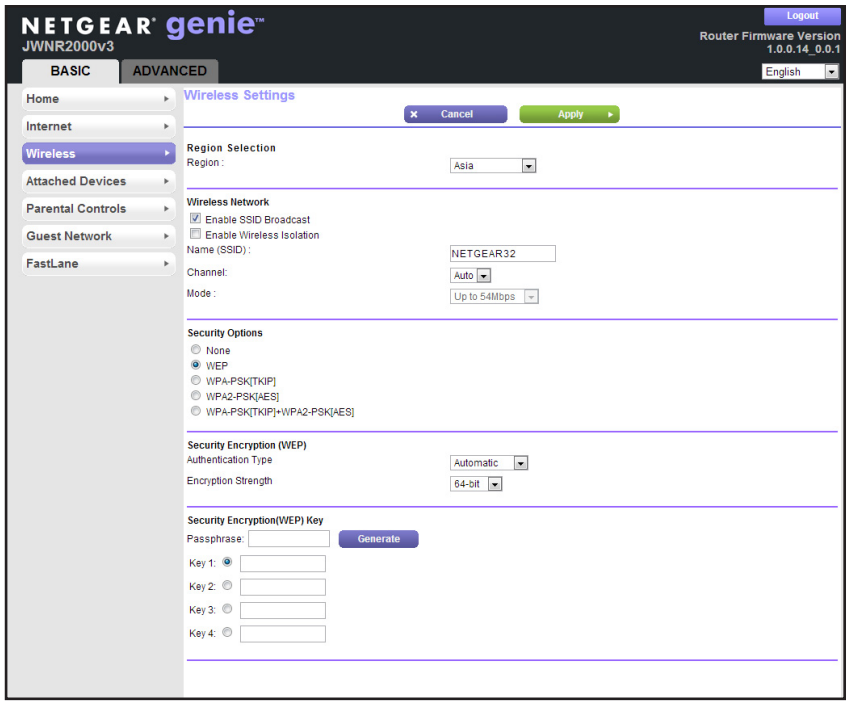
You can change the WEP security settings for your router. If you do so, then write down the new settings and store them in a secure place for future reference. For more information about WEP, see *WEP Encryption* on page 29.

➢ **To change the WEP settings:**

1. Select **BASIC > Wireless**.

   The Wireless Setup screen displays.

2. In the Security Options section, select **WEP**:



3. Select the authentication type.

   The default is Automatic. Other choices are Open System (any client can authenticate itself to the network) and Shared Key (a passphrase and a four-way challenge are needed for authentication).

4. Select the encryption strength setting, either 64 bit or 128 bit.
5. Enter the four data encryption keys either manually or automatically.

   These values have to be identical on all computers and access points in your network.

   - **Automatic**. Enter a word or group of printable characters in the Passphrase field, and click **Generate**. The four key fields are automatically populated with key values.
   - **Manual**. The number of hexadecimal digits that you enter depends on the encryption strength setting:
     - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
     - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).

6. Select the radio button for the key you want to make active.

   Make sure that you understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one in Windows XP allow one key entry, which has to match the default key you set in the router.

7. Click **Save** to save your settings, or click **Apply** so your changes to take effect immediately.

Change the WPA Security Option and Passphrase

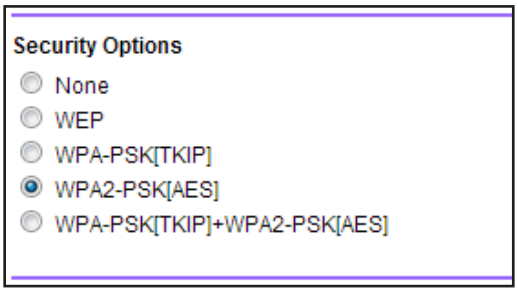
You can change the WPA security settings for your router. If you do so, then write down the new settings and store them in a secure place for future reference. For more information about WPA, see *WPA Encryption* on page 29.

➢ **To change the WPA security option and password:**

1. Select **BASIC > Wireless**.

   The Wireless Settings screen displays.

2. Under Security Options, select a WPA option.



3. In the PassPhrase field that displays when you select a WPA security option, enter the network key (password) that you want to use.

   It is a text string from 8 to 63 characters.

View Attached Devices

You can view all computers or devices that are currently connected to your network from the Attached Devices screen.

From the BASIC Home screen, select **Attached Devices**.

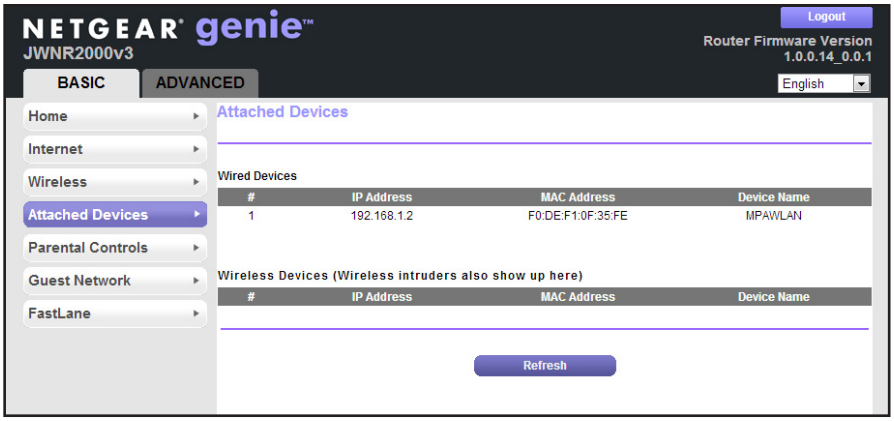


Figure 9. Attached Devices Screen

Wired devices are connected to the router with Ethernet cables. Wireless devices have joined the wireless network. NETGEAR genie displays the following information about devices that are currently connected to your 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 if a device is disconnected and rejoins the network.
- **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.
- **Device Name**. If the device name is known, it is shown here.

Click **Refresh** to update this screen.

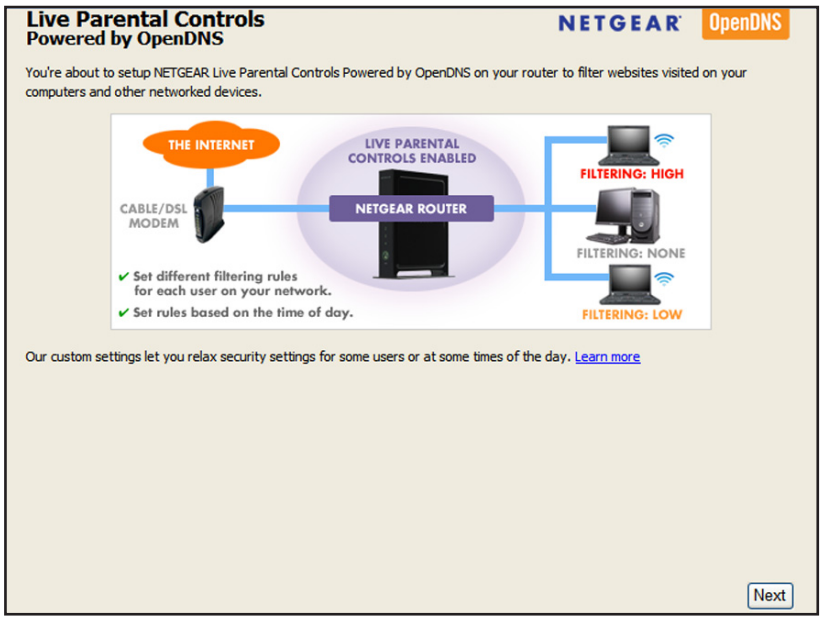
Parental Controls

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

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

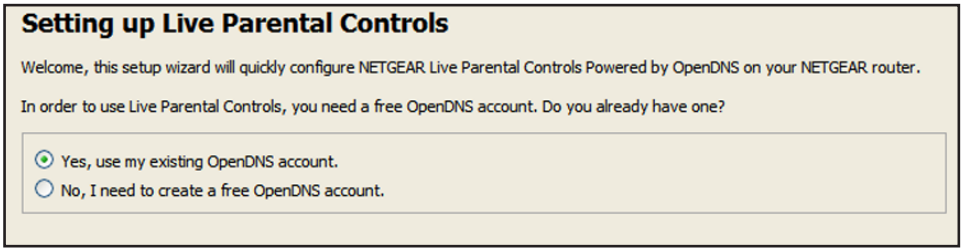
1. From the BASIC Home screen, select **Parental Controls** to go to the Live Parental Controls website.
2. Click either the **Windows Users** or **Mac Users** button on the website.
3. Follow the onscreen instructions to download and install the NETGEAR Live Parental Controls Management Utility.

After installation, Live Parental Controls automatically starts.



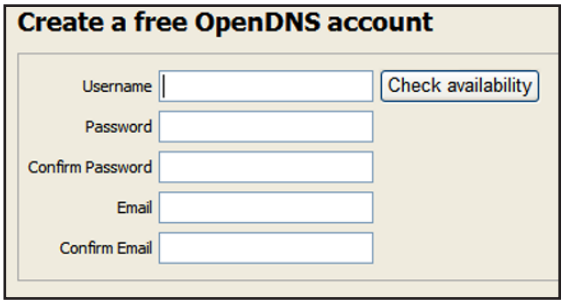
4. Click **Next**, read the note, and click **Next** again.

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



5. Select the radio button that applies to you, as follows, 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.

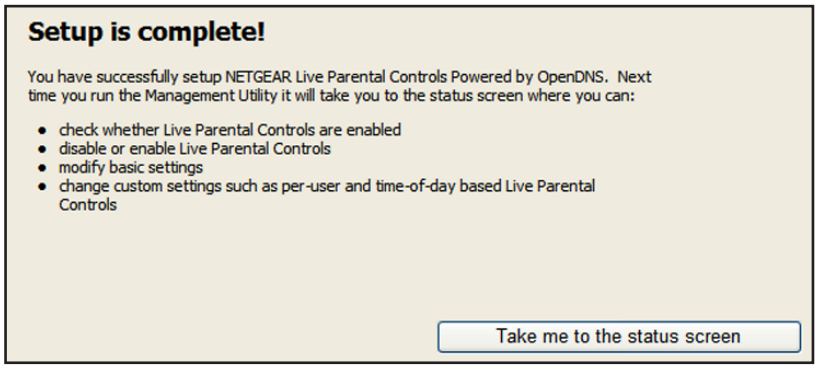
     If you are creating an account, the following screen displays:



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

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

6. Select a filtering level radio button and click **Next**.



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

   Parental controls are now set up for the router. The BASIC Home screen shows Parental Controls as enabled.

➢ **To manage existing Live Parental Controls:**

1. From the BASIC Home screen, select **Parental Controls** to open the Parental Controls Center login screen.

2. Use your OpenDNS account to log in and manage your Live Parental Controls settings.

Set Up a Guest Network

Adding a guest network allows visitors at your home to use the Internet without giving them your wireless security key. You can add a guest network to the 2.4 GHz b/g/n wireless network.

➢ **To set up a guest network:**

1. From the BASIC Home screen, select **Guest Network**.

   The following screen:

2. Select any of the following wireless settings:
   - **Enable Guest Network**. When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.
   - **Enable SSID Broadcast**. If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.
   - **Allow Guest to access My Local Network**. If this check box is selected, anyone who connects to this SSID has access to your local network, not just Internet access.
   - **Enable Wireless Isolation**. If this check box is selected, wireless computers or devices that join the network can use the Internet but cannot access each other or access Ethernet devices on the network.
3. Give the guest network a name.

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

   The security options are described in *Security Options* on page 28.
5. Click **Apply**.

   Your settings are saved.

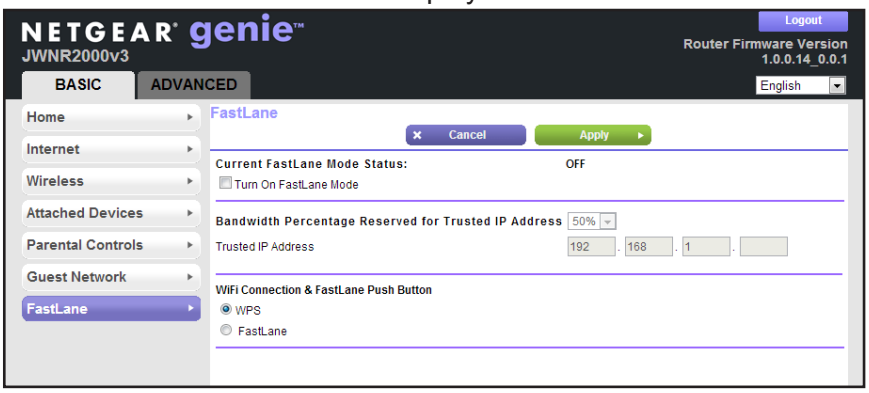
Set Up FastLane

You can use the FastLane feature to reserve bandwidth on the router for a trusted IP address that you specify. The first time you turn on FastLane, you should specify the amount of bandwidth you want to reserve and set up the WPS/FastLane button for FastLane.

FastLane prevents others from using up your bandwidth. When you connect to the router from the trusted IP address, you have guaranteed bandwidth for video steaming applications.

➢ **To set up the FastLane feature:**

1. Select **BASIC > FastLane** to display the FastLane screen:



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

By default, FastLane is turned off, and WPS is turned on.

3. Select the amount of bandwidth to be reserved from the drop-down menu.

   You can choose to reserve 50%, 60%, 70%, or 80% of the bandwidth.

4. Enter the trusted IP address.
5. Select the **FastLane** radio button.
6. Click **Apply**.

After you set up the FastLane feature, you can use the WPS/FastLane button on the back of the router to turn FastLane on or off (see *Figure 3, Back panel* on page 9).

Note: By default, the WPS/FastLane button is set up for WPS.

➢ **To change the WPS/FastLane button configuration:**

1. Select **BASIC > FastLane** to display the FastLane screen.
2. Select either the **WPS** or **FastLane** radio button.
3. Click **Apply**.

genie Advanced Home

4

Specifying custom settings

This chapter contains the following sections:

Some selections on the ADVANCED tab are described in separate chapters:

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

NETGEAR genie ADVANCED Home Screen

The genie ADVANCED Home dashboard present status information. The content is the same as what is on the Router Status screen available from the Administration menu. For more information about the Router Status screen, see *View Router Status* on page 62.

The genie ADVANCED Home screen is shown in the following figure:

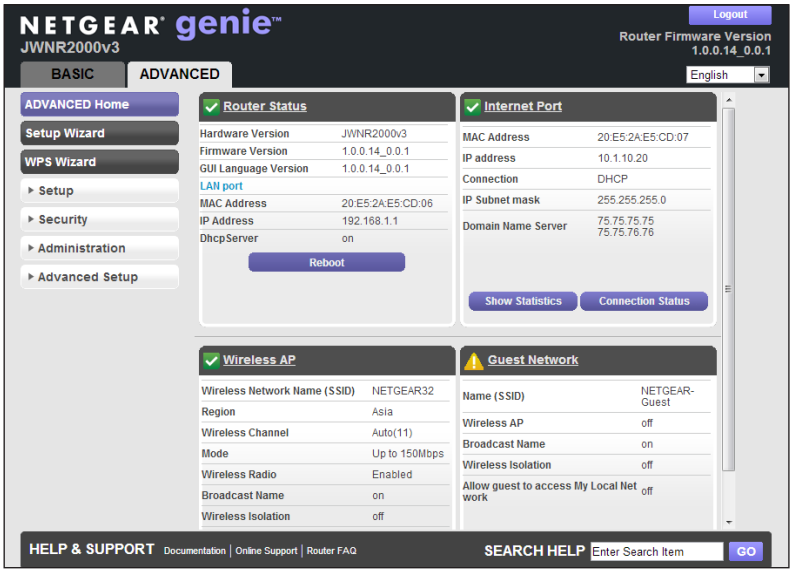


Figure 10. genie ADVANCED Home screen

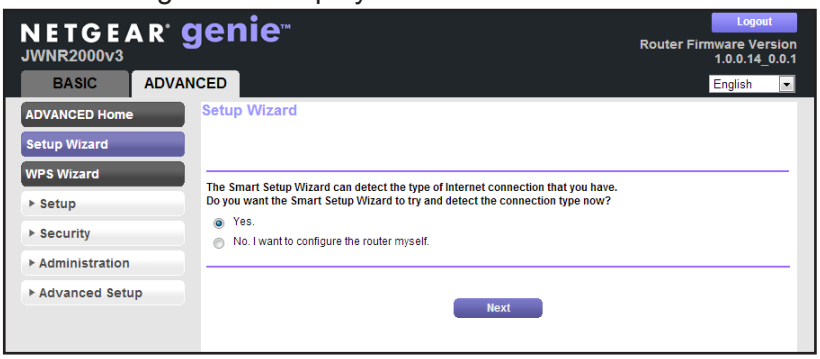
Setup Wizard

The NETGEAR genie installation process launches the first time you set up the router. After you set up the router for the first time, you can use the Setup Wizard to automatically detect your ISP configuration.

➢ **To use the Setup Wizard:**

1. Log in to the router and click the **ADVANCED** tab.
2. Select **Setup Wizard**.

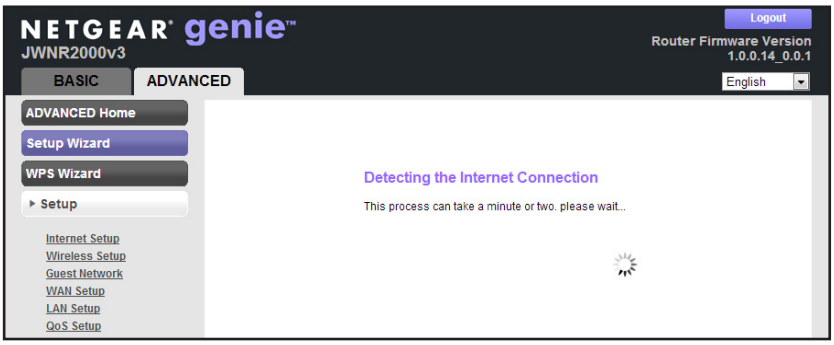
   The following screen displays.



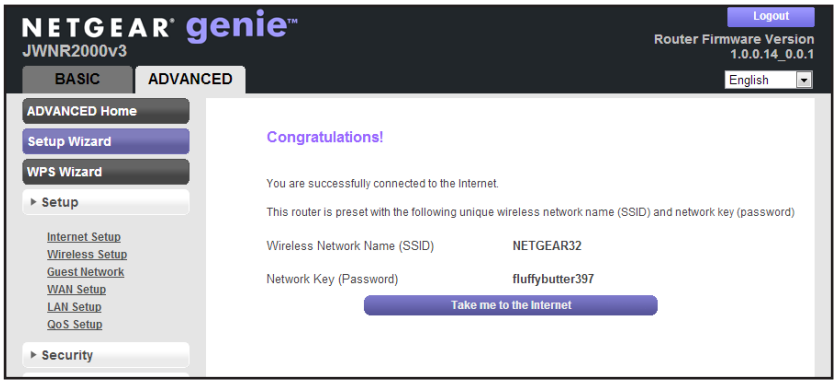
3. Select the **Yes** radio button and click **Next**.

   If you select No, you are taken to the BASIC Settings screen (see *Basic Settings* on page 23).

   The following screen displays:



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

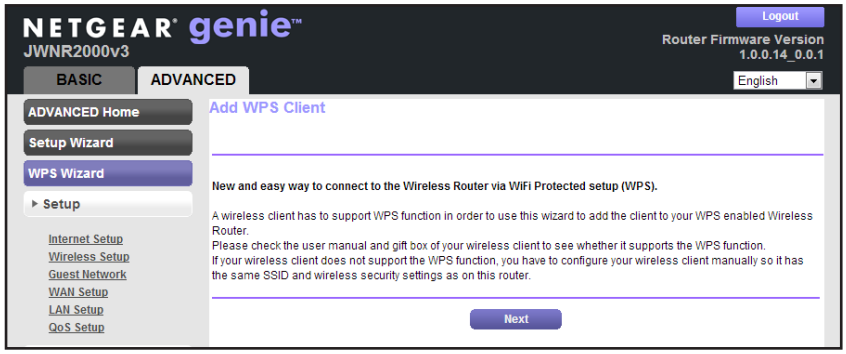


WPS Wizard

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

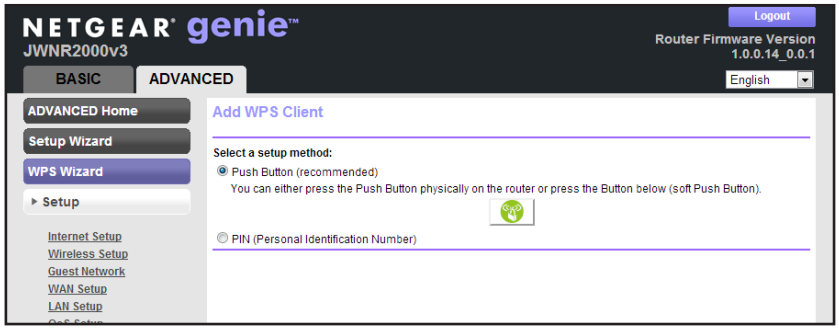
➢ **To use the WPS Wizard:**

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



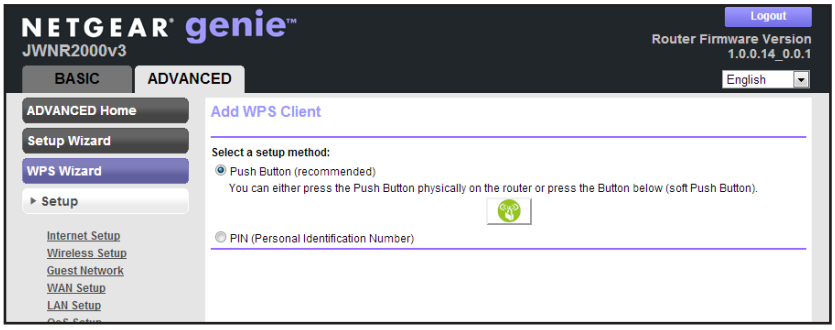
2. Click **Next**.

   The following screen lets you select the method for adding the WPS client (a wireless device or computer).



3. Select either **Push Button** or **PIN**, as follows:

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



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

The router attempts to add the WPS-capable device. The WPS/FastLane 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. (Optional) 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:

- **Internet Setup**. This selection is a shortcut to the same Basic Settings screen that you can access from the BASIC Home screen. See *Basic Settings* on page 23.
- **Wireless Setup**. This selection is a shortcut to the same Wireless Settings screen that you can access from the BASIC Home screen. See *Basic Wireless Settings* on page 26.
- **Guest Network**. This selection is a shortcut to the same Guest Network screen that you can access from the BASIC Home screen. See *Set Up a Guest Network* on page 35.
- **WAN Setup**. Internet (WAN) setup. See *WAN Setup* on page 42.
- **LAN Setup**. Local area network (LAN) setup. See *LAN Setup* on page 46.
- **QoS Setup**. Quality of Service (QoS) setup. See *Quality of Service (QoS) Setup* on page 49.

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:

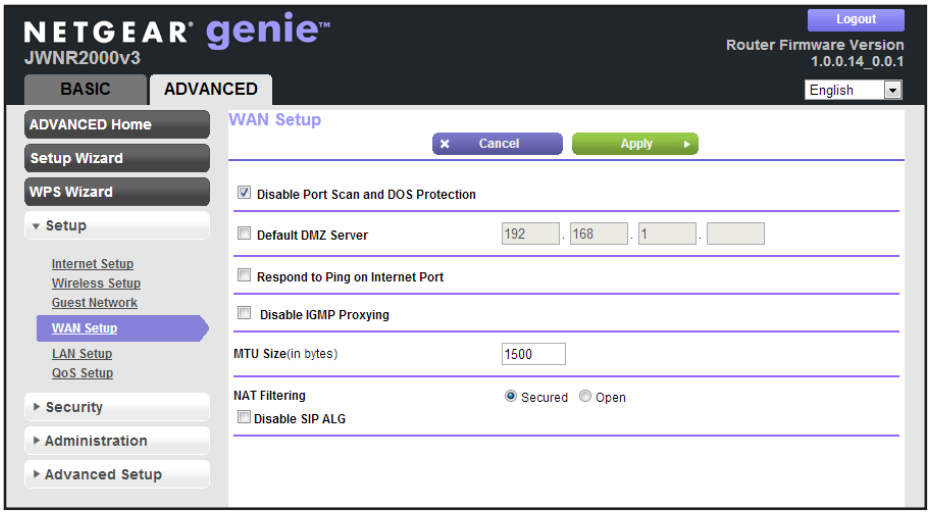


Figure 11. WAN Setup screen

You can configure the following settings:

- **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. Use this setting only in special circumstances.
- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, *Default DMZ Server*, for more details.
- **Respond to Ping on Internet Port**. If you want the router to respond to a ping from the Internet, select this check box. Use this feature only as a diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.
- **Disable IGMP Proxying**. IGMP proxying allows a computer on the local area network (LAN) to receive the multicast traffic it is interested in from the Internet. If you do not need this feature, you can select this check box to disable it.
- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. Reducing the MTU 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 44.
- **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 it allows almost all Internet applications to function.
- **Disable SIP ALG**. Some SIP (Session Initiation Protocol) applications have their own way to work around the NAT firewall issue, and the SIP ALG (Application Layer Gateway) would conflict with those solutions. In most cases, you do not have to disable the SIP ALG. However, if your SIP applications cannot work with the router, you can disable the SIP ALG and try the applications again. Select the check box to disable SIP ALG.

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

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

   The WAN Setup screen displays.

2. Specify the settings for your Internet connection.

   For more information about the settings, see *WAN Setup* on page 42.

3. Click **Apply**.

Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The router is programmed to recognize some of these applications and to work

correctly with them, but other applications might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

WARNING:

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

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

➢ **To set up a default DMZ server:**

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

   The WAN Setup screen displays.

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

   Your changes are saved.

Change the MTU Size

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

The best MTU setting for NETGEAR equipment is often the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that does not open, or displays only part of a web page
  - Yahoo email
  - MSN portal

  - America Online's DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

Note: An incorrect MTU setting can cause Internet communication problems. For instance, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

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

Table 2. Common MTU sizes

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

   The WAN Setup screen displays.

2. In the MTU Size field, enter a value from 64 to 1500.
3. Click **Apply**.

   Your change is saved.

LAN Setup

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

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

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

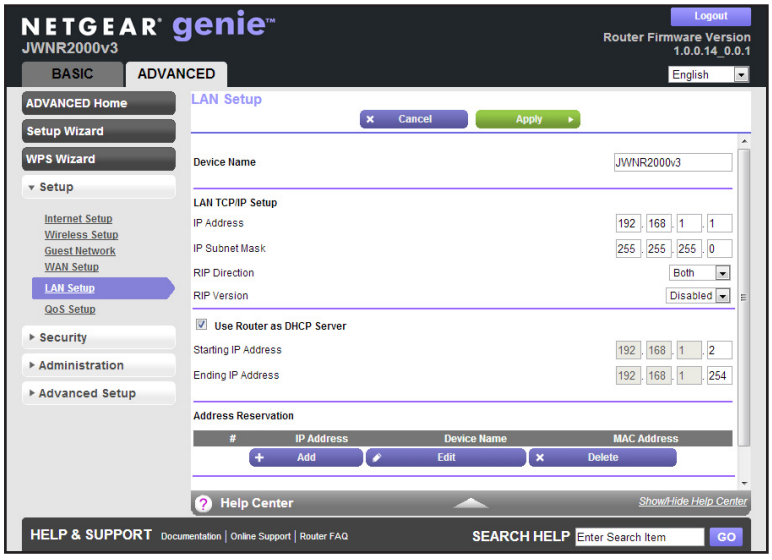
These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings in the LAN Setup screen.

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

➢ **To change the LAN settings:**

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

   The LAN Setup screen displays:



2. Enter the settings that you want to customize.

   These settings are described in the following section, *LAN Setup Screen Settings*.

3. Click **Apply**.

   Your changes are saved.

LAN Setup Screen Settings

You can configure the following LAN settings:

- **Device Name**. This is the abbreviated name of the modem router.
- **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 must 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 by default 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 acts as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers from a pool of addresses specified in 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.

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 Basic Settings screen; otherwise, the router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Basic Settings screen)

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

1. Select **ADVANCED > Setup > LAN Setup**.
2. Make sure that the **Use Router as DHCP Server** check box is selected.
3. Specify the range of IP addresses.

   For example, using the default addressing scheme, define a range between 192.168.1.2 and 192.168.1.254, although you might want to save part of the range for devices with fixed addresses.

   - In the Starting IP Address field, specify the start of the range for the pool of IP address in the same subnet as the modem router.
   - In the Ending IP Address field, specify the end of the range for the pool of IP address in the same subnet as the modem router.
4. Click **Apply**.

   Your changes are saved.

➢ **To disable the DHCP Server feature in the modem router:**

1. Select **ADVANCED > LAN Setup**.
2. Clear the **Use Router as DHCP Server** check box.
3. Click **Apply**.
4. If no DHCP server is on your network, set your computers' IP addresses manually so that they can access the modem router.

Address Reservation

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

➢ **To reserve an IP address:**

1. Select **ADVANCED > Setup > LAN Setup**.
2. In the Address Reservation section of the screen, click the **Add** button.

   The Address Reservation screen displays.
3. If the device is in the Address Reservation Table, select its radio button.

   The information from the Address Reservation Table populates the IP Address, MAC Address, and Device Name fields.

If the device is not in the list, click **Refresh**. If it still does not appear, fill in these fields manually.

a. 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.)

b. In the MAC Address field, 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.

c. In the Device Name field, type the name of the computer or server.

4. Click **Apply**.

The reserved address is entered into the list.

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**.

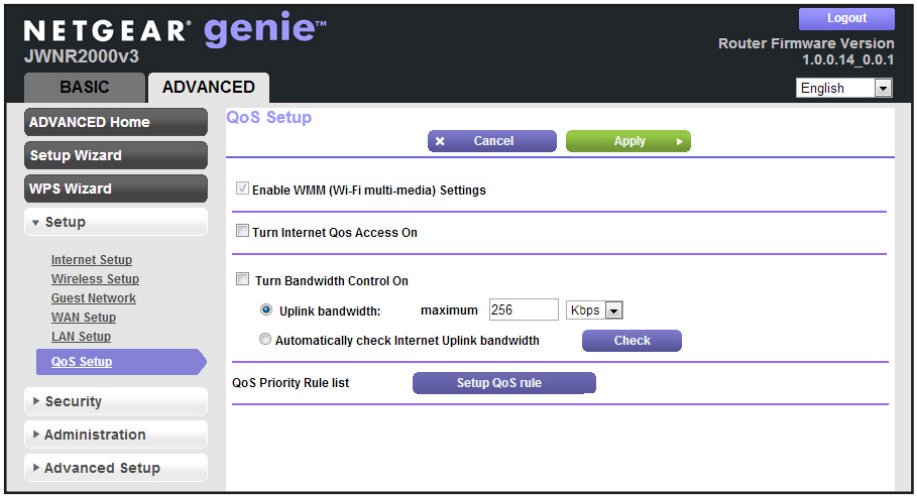
Quality of Service (QoS) Setup

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**.

The following screen displays:



Enable WMM QoS for Wireless Multimedia Applications

The router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both the application and the client running that application must have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen by clearing the **Enable WMM** check box and clicking **Apply**.

Set Up QoS for Internet Access

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

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

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

Set Up QoS for Applications and Online Gaming

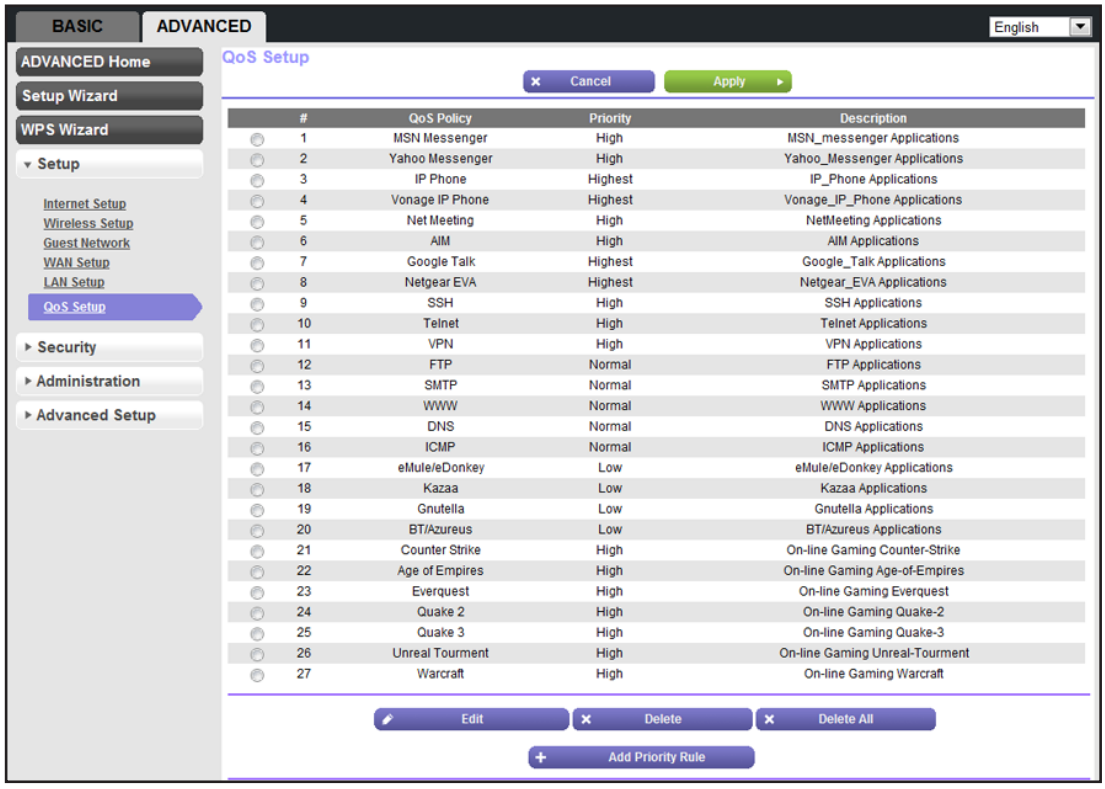
➢ **To create a QoS policy for applications and online games:**

1. Select **ADVANCED > Setup > QOS Setup**.

   The QOS Setup screen displays.

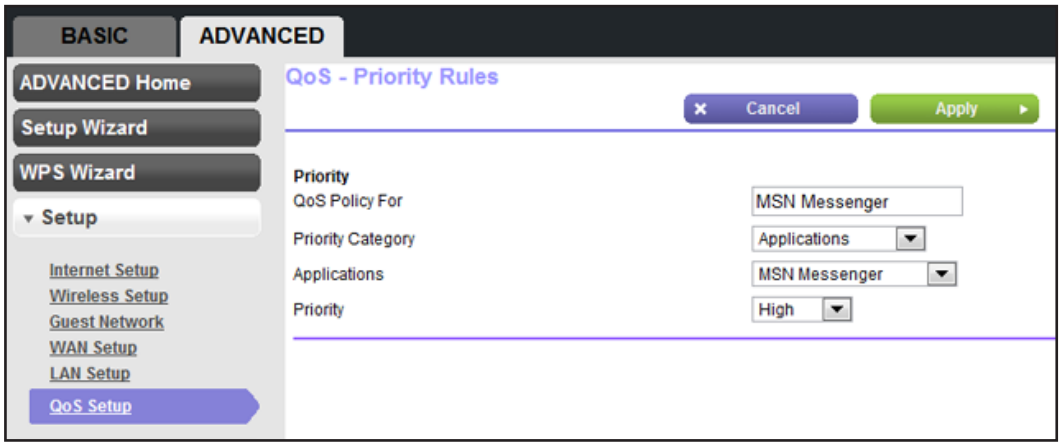
2. Select the **Turn Internet Access QoS On** check box.
3. Click **Apply**.
4. Click the **Setup QoS Rule** button.

The existing priority rules displays:



5. To add a priority rule, scroll down to the bottom of the screen and click **Add Priority Rule**.

   The Qos - Priority Rules screen displays:

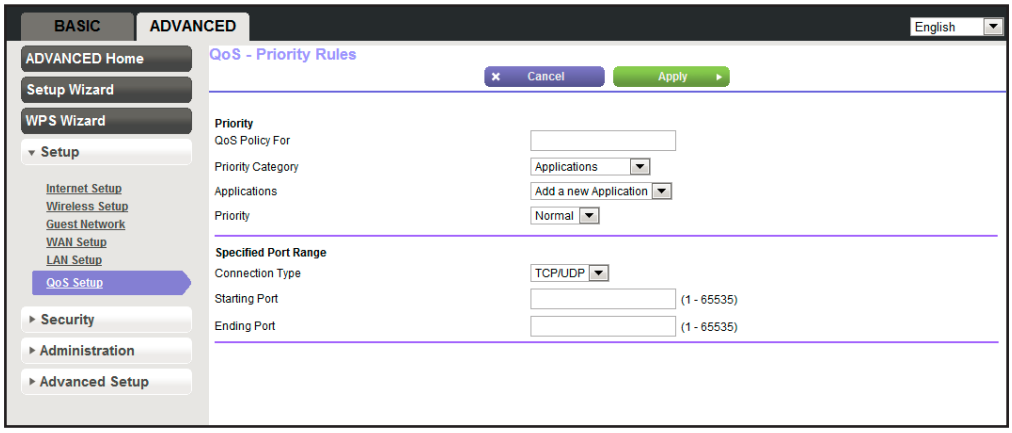


6. From the Priority Category drop-down menu, select either **Applications** or **On-line Gaming**.

   The Applications or On-line Gaming drop-down menu displays.

7. Select an existing application or game entry from the drop-down menu, or scroll and select **Add a New Application** or **Add a New Game,** as applicable.

   If you add an entry, the Priority Rules screen expands as shown:



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

   b. From the Connection Type drop-down menu, select either **TCP**, **UDP**, or both (**TCP/UDP**). Specify the port number or range of port numbers that the application or game uses.

8. From the Priority drop-down menu, select the priority for Internet access for this traffic relative to other applications and traffic.

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

9. Click **Apply**.

   This rule is saved to the QoS Policy table.

Set Up QoS for a Router LAN Port

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

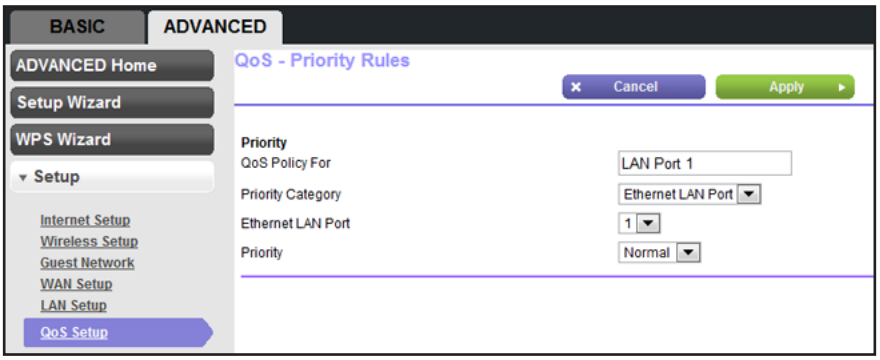
1. Select **Advanced > Setup > QoS Setup**.

   The QoS Setup screen displays.

2. Select the **Turn Internet Access QoS On** check box and click **Apply**.
3. Click the **Setup QoS Rule** button to see the existing priority rules.
4. Scroll down to the bottom of the screen and click the **Add Priority Rule** button.

   The Qos - Priority Rules screen displays.

5. From the Priority Category drop-down menu, select **Ethernet LAN Port**.



6. From the Ethernet LAN Port drop-down menu, select the LAN port.
7. From the Priority drop-down menu, select the priority for Internet access for this port's traffic relative to other applications.

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

8. Click **Apply**.

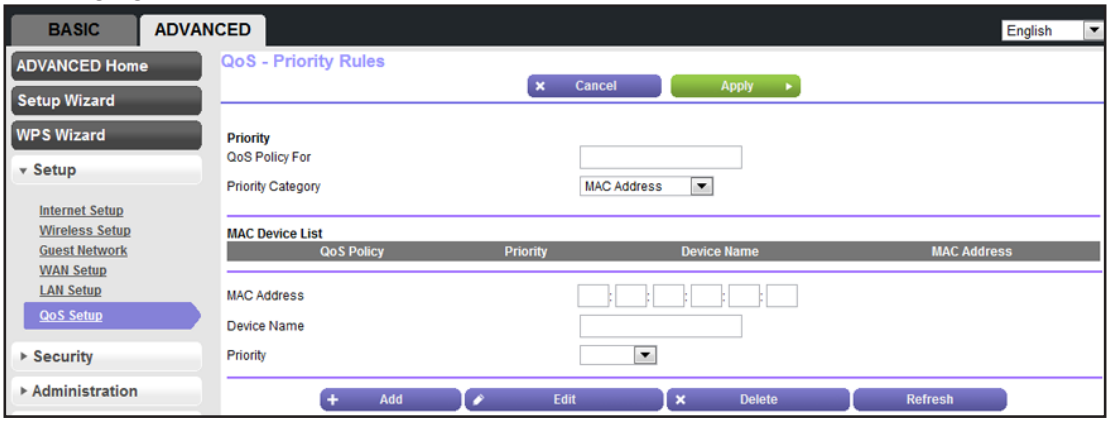
   This rule is saved to the QoS Policy table.

Set Up QoS for a MAC Address

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

1. Select **ADVANCED > Setup > QoS Setup** to display the QoS Setup screen.
2. Select the **Turn Internet Access QoS On** check box and click **Apply**.
3. Click the **Setup QoS Rule** button to see the existing priority rules.
4. Scroll down to the bottom of the screen and click the **Add Priority Rule** button.
   The Qos - Priority Rules screen displays.

5. From the Priority Category drop-down menu, select **MAC Address**, as shown in the following figure:



6. If the device is in the MAC Device List, select its radio button.

   The information from the MAC Device List populates the QoS Policy For, MAC Address, and Device Name fields.

   If the device is not in the list, click **Refresh**. If it still does not appear, fill in these fields manually.

7. From the Priority drop-down menu, select the priority for Internet access for this device's traffic relative to other applications and traffic.

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

8. Click **Apply** to save this rule to the QoS Policy table.

Edit or Delete an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

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

   The QoS Setup screen displays.

2. Click the **Setup QoS Rule** button.
3. Select the radio button next to the QoS policy that you want 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.
4. Click **Apply**.

   Your changes are saved.

You can also delete all of the rules by simply clicking the **Delete All** button below the QoS Policy table.

Security

5

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 devices on your network. These features are available from the Security menu on the genie ADVANCED tab.

This chapter includes the following sections:

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

The Parental Controls selection on the Security menu of the genie ADVANCED tab is described in *Parental Controls* on page 32.

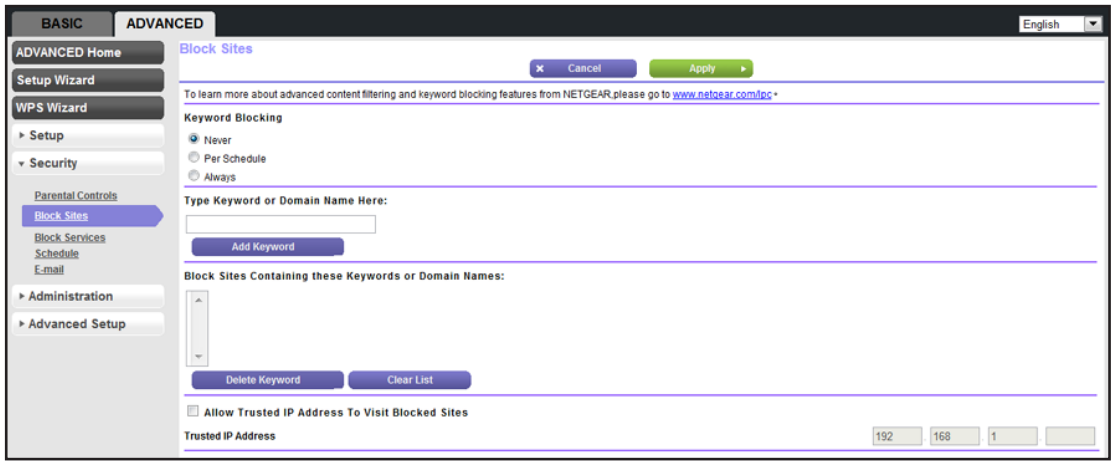
Keyword Blocking of HTTP Traffic

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

➢ **To set up keyword blocking:**

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

   The following screen displays:



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.

   If you selected Per Schedule, specify a time period in the Schedule screen. For more information, see *Schedule Blocking* on page 59.

3. In the Keyword field, enter a keyword or domain.

   The Keyword list supports up to 32 entries. Following are 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.

4. Click **Add Keyword**.
5. Click **Apply**.

➢ **To delete a keyword or domain:**

1. Select the keyword you want to delete from the list.
2. Click **Delete Keyword**.
3. Click **Apply**.

   You changes are saved.

➢ **To specify a trusted computer:**

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

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply**.

   Your changes are saved.

Block Services (Port Filtering)

Services are functions that server computers perform at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, 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.

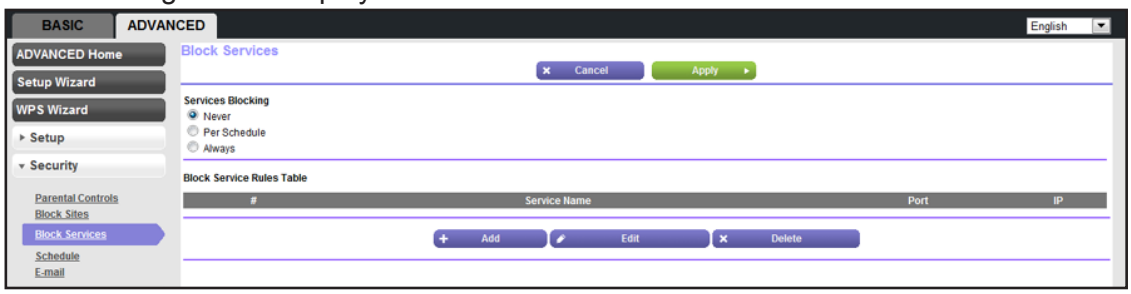
The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024–65535 by the authors of the application. Although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

   The following screen displays:

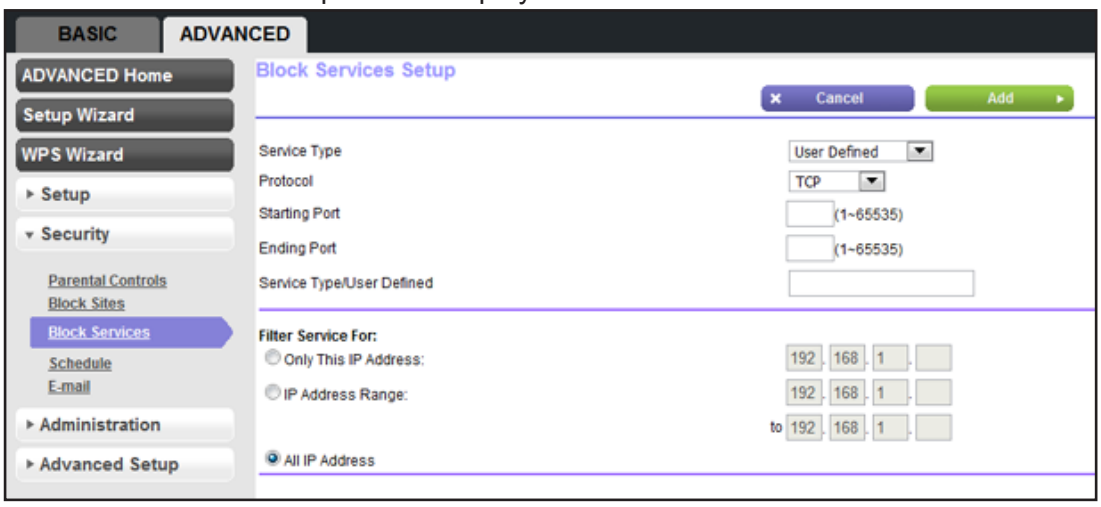


2. Select either **Per Schedule** or **Always** to enable service blocking, and click **Apply**.

   If you selected Per Schedule, specify a time period in the Schedule screen. For more information, see *Schedule Blocking* on page 59.

3. Click **Add** to add a service.

   The Block Services Setup screen displays:



4. From the Service Type drop-down menu, select the application or service to allow or block.

   The menu 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. From the Protocol drop-down menu, select **TCP**, **UDP**, or **TCP/UDP**.

   If you know that the application uses either TCP or UDP, select the appropriate protocol.

   If you are not sure, select **TCP/UDP**.

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.

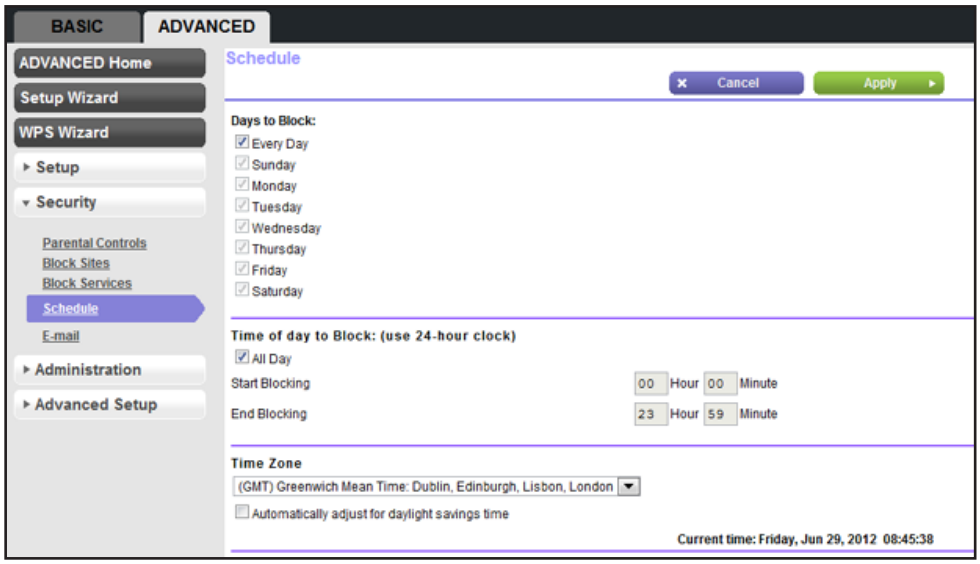
Schedule Blocking

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

➢ **To schedule blocking:**

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

   The following screen displays:



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 drop-down menu.
4. If you use daylight saving time, select the **Automatically adjust for daylight savings time** check box.
5. Click **Apply**.

   Your settings are saved.

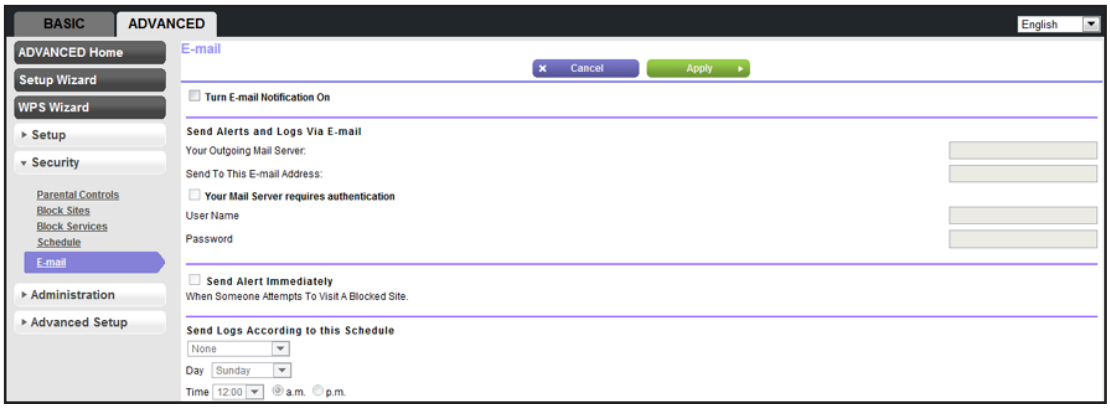
Security Event Email Notifications

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**.

   The followings screen displays.



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's outgoing (SMTP) mail server (such as mail.myISP.com).

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

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

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

5. If your outgoing email server requires authentication, select the **Your Mail Server requires authentication** check box, and fill in the User Name and Password fields for the outgoing email server.
6. To have email alerts sent immediately when someone attempts to visit a blocked site, select the **Send Alert Immediately** check box.
7. (Optional) Establish a log email schedule.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is 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.

8. Click **Apply**.

   Your settings are saved.

Administration

6

Managing your network

This chapter describes the router settings for administering and maintaining your router and home network. These settings are available from the Administration menu on the genie ADVANCED tab. For information about checking the status of your router over the Internet, see *Remote Management* on page 93. For information about monitoring Internet traffic on your router's Internet port, see *Traffic Meter* on page 95.

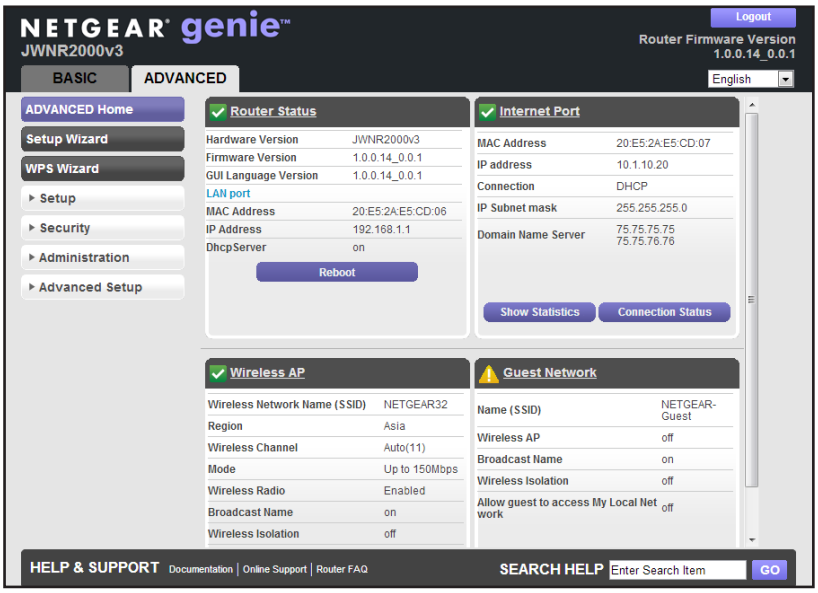
This chapter includes the following sections:

- *View Router Status*
- *View Logs of Web Access or Attempted Web Access*
- *Manage the Configuration File*
- *Change the Password*
- *Upgrade the Router Firmware*

The Attached Devices selection in the Administration menu is described in *View Attached Devices* on page 31.

View Router Status

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



This screen is also displayed through the Advanced Home menu.

For information about the Guest Network section of the screen, see *Set Up a Guest Network* on page 35.

Router Status

The Router Status section provides the following information:

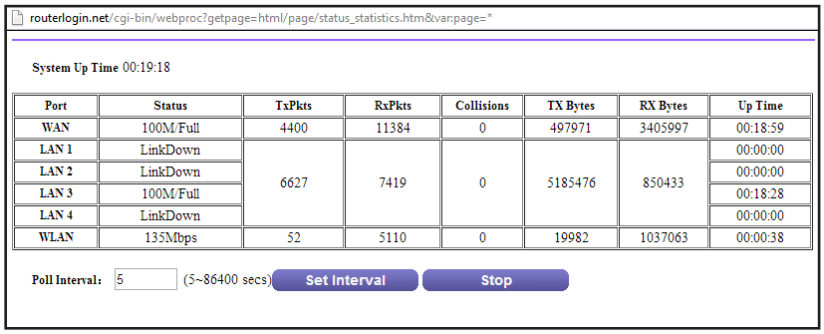
- **Hardware Version**. The router model.
- **Firmware Version**. The version of the router firmware. It changes if you upgrade the router firmware.
- **GUI Language Version**. The localized language of the user interface.
- **MAC Address**. The Media Access Control (MAC) address is the unique physical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

Internet Port

The Internet Port section provides the following information:

- **MAC Address**. The Media Access Control (MAC) address, which is the unique physical address that the Internet (WAN) port of the router uses.

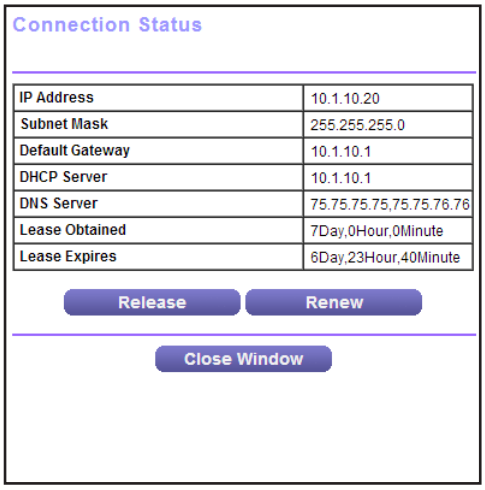
- **IP Address**. The IP address that the Internet (WAN) port of the router uses. If no address is shown or the address is 0.0.0, the router cannot connect to the Internet.
- **Connection**. This shows if the router is using a fixed IP address on the WAN. If the value is DHCP Client, the router obtains an IP address dynamically from the ISP.
- **IP Subnet Mask**. The IP subnet mask that the Internet (WAN) port of the router uses.
- **Domain Name Server**. The Domain Name Server addresses that the router uses. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.
- **Show Statistics button**. Click the **Show Statistics** button to display the following screen:



The Show Statistics screen provides the following information:

- **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 the following information:
  - **Status**. The link status of the port.
  - **TxPkts**. The number of packets transmitted on this port since reset or manual clear.
  - **RxPkts**. The number of packets received on this port since reset or manual clear.
  - **Collisions**. The number of collisions on this port since reset or manual clear.
  - **Tx B/s**. The current transmission (outbound) bandwidth used on the WAN and LAN ports.
  - **Rx B/s**. The current reception (inbound) bandwidth used on the WAN and LAN ports.
  - **Up Time**. The time elapsed since this port acquired the link.
  - **Poll Interval**. The interval at which the statistics are updated in this screen. To change the polling frequency, enter a time in seconds in the Poll Interval field, and click **Set Interval**. To stop the polling entirely, click **Stop**.

- **Connection Status button**. Click the **Connection Status** button to view connection status information.



The Connection Status screen displays the following information:

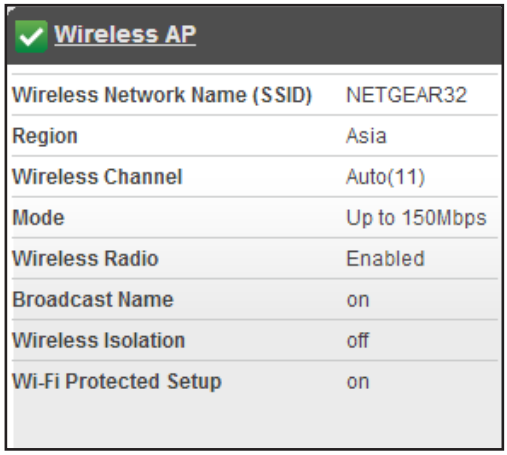
- **IP Address**. The IP address that is assigned to the router.
- **Subnet Mask**. The subnet mask that is assigned to the router.
- **Default Gateway**. The IP address for the default gateway that the router communicates with.
- **DHCP Server**. The IP address for the Dynamic Host Configuration Protocol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

The Release button returns the status of all items to 0.

The Renew button refreshes the items.

The Close Window button closes the Connection Status screen.

Wireless AP



The Wireless AP section displays the following information:

- **Wireless Network Name (SSID)**. The wireless network name (SSID) that the router uses.
- **Region**. The geographic region where the router is being used. It might be illegal to use the wireless features of the router in some parts of the world.
- **Wireless Channel**. Identifies the operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the router finds the best operating channel available. If you notice interference from nearby devices, you can select a different channel. Channels 1, 6, and 11 do not interfere with each other.
- **Mode**. Indicates the wireless communication mode: Up to 54 Mbps, Up to 150 Mbps (default), or Up to 300 Mbps.
- **Wireless Radio**. Indicates whether the radio feature of the router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.
- **Broadcast Name**. Indicates whether the router is broadcasting its SSID.
- **Wireless Isolation**. Indicates whether devices that join your network can access each other and Ethernet devices on the network.
- **Wi-Fi Protected Setup**. Indicates whether Wi-Fi Protected Setup is configured for this network.

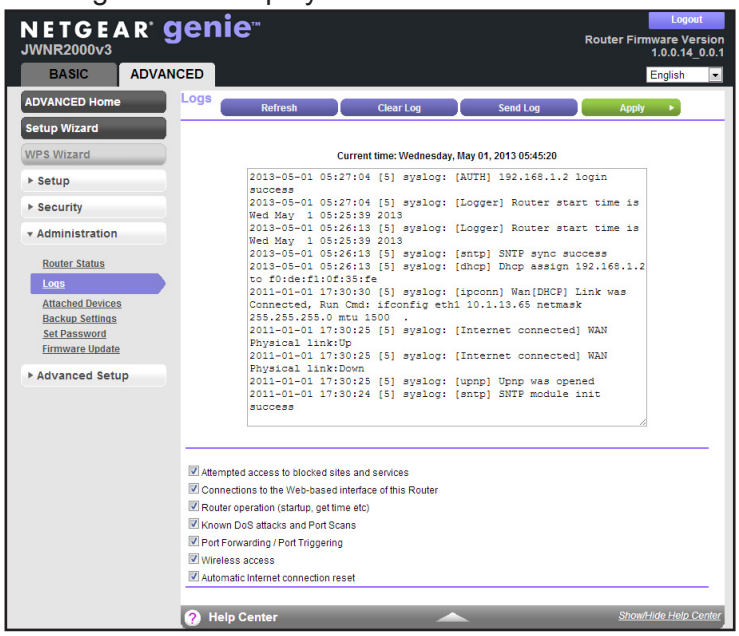
View Logs of Web Access or Attempted Web Access

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

➢ **To view web access logs:**

Select **ADVANCED > Administration > Logs**.

The Logs screen displays.



The Logs screen shows the following information:

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

The Refresh button refreshes the Logs screen. The Clear Log button clears the log entries. The Send Log button emails the log immediately.

The following events can be included in the log:

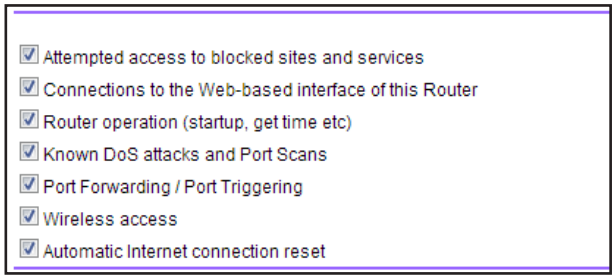
- **Attempted access to blocked sites**. If selected, attempted Internet accesses that were blocked are logged.
- **Connections to the Web-based interface of this Router**. If selected, the log tracks each time someone logs in to the router.
- **Router operation (startup, get time etc)**. If selected, router operations not covered by the preceding selections are logged.
- **Known DoS attacks and Port Scans**. If selected, denial of service attacks, as well as port scans, are logged.
- **Port Forwarding / Port Triggering**. If selected, the port forwarding or port triggering attempts are logged.
- **Wireless access**. If selected, attempts to access the wireless are logged.
- **Automatic Internet connection reset**. If selected, any automatic reset of the internet connection are logged.

➢ **To include events in the log:**

1. Select **ADVANCED > Administration > Logs**.

   The Logs screen displays.

2. Select the check box of the events you want to include in the log.



   Selecting all check boxes increases the size of the log, so it is good practice to disable any events that are not really required.

3. Click **Apply**.

   Your changes are saved.

Manage the Configuration File

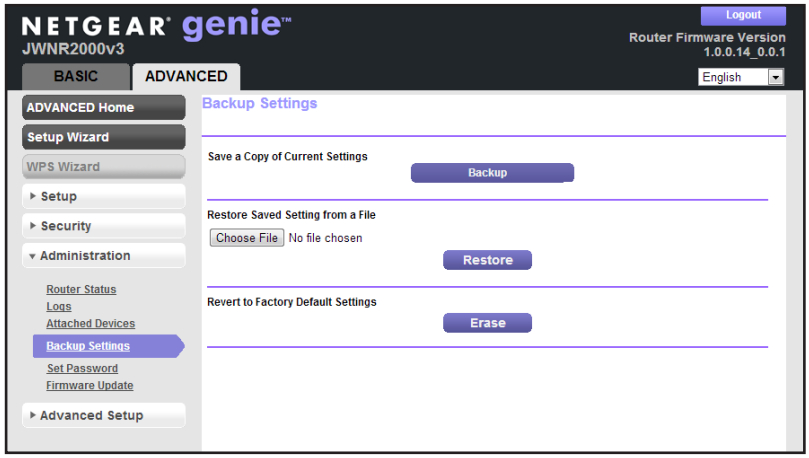
The configuration settings of the router are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

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

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

   The following screen displays:



2. Click **Backup**.

   A copy of the current settings is saved.

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

   The Backup Settings screen displays.

2. Click the **Browse** button to find the .cfg file, and select it.
3. Click the **Restore** button.

   The file is uploaded to the router.

   Upon completion, the router reboots.

WARNING:

Do not interrupt the reboot process.

Erase the Current Configuration Settings

You can erase the configuration and restore the factory default settings. If you move the router to a different network or if you forget the password, you might want to restore factory default settings.

You can use the Reset button on the back of the router (see *Factory Settings* on page 108), or you can click the **Erase** button on the Backup Settings screen. For more information, see the following procedure.

➢ **To erase the configuration settings and reset the router to the factory default settings:**

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

   The Backup Settings screen displays.

1. Click **Erase**.

Note: 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.

Change the Password

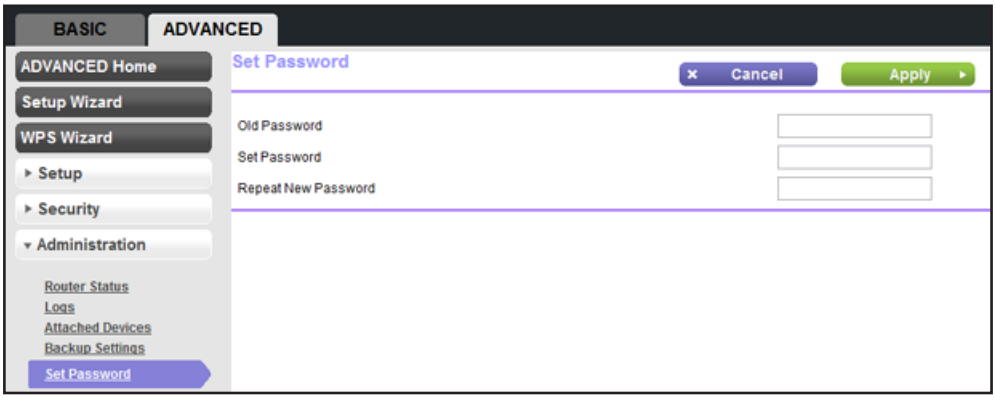
This feature allows you to change the default password that is used to log in to the router with the user name admin.

Note: This procedure 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 *Label* on page 7).

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

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

   The following screen displays:



2. Type the old password in the Old Password field.
3. Type the new password in the Set Password field and in the Repeat New Password field.
4. Click **Apply**.

   Your changes take effect.

Upgrade the Router Firmware

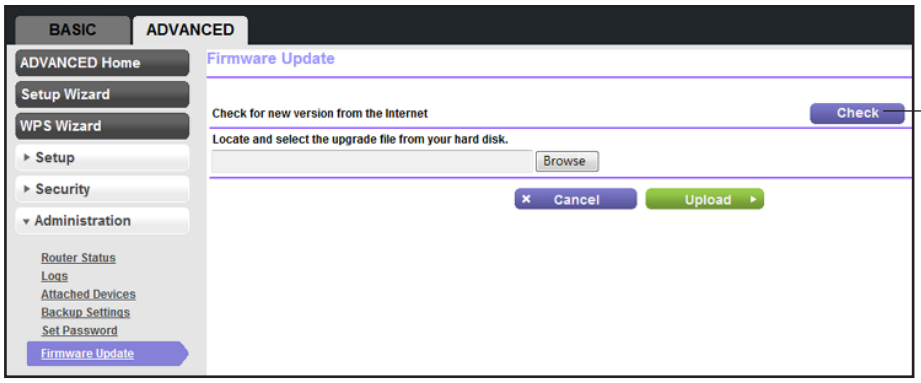
The router firmware (routing software) is stored in flash memory. You can update the firmware from the Administration menu on the ADVANCED tab. You might see a message at the top of the genie screens when new firmware is available for your product.

You can use the Check button on the Firmware Update 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 > Firmware Update**.

   The following screen displays:



2. Click the **Check** button.

   If new firmware is available, the router finds it.

3. Click **Yes**.

   The router locates the firmware you downloaded (the file ends in .img) and begins the update.

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 one minute. Read the new firmware release notes to determine whether you need to reconfigure the router after upgrading.

7. Advanced Settings

This chapter describes the advanced features of your router. The information is for readers with advanced networking knowledge who want to configure the router for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter includes the following sections:

Advanced Wireless Settings

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

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

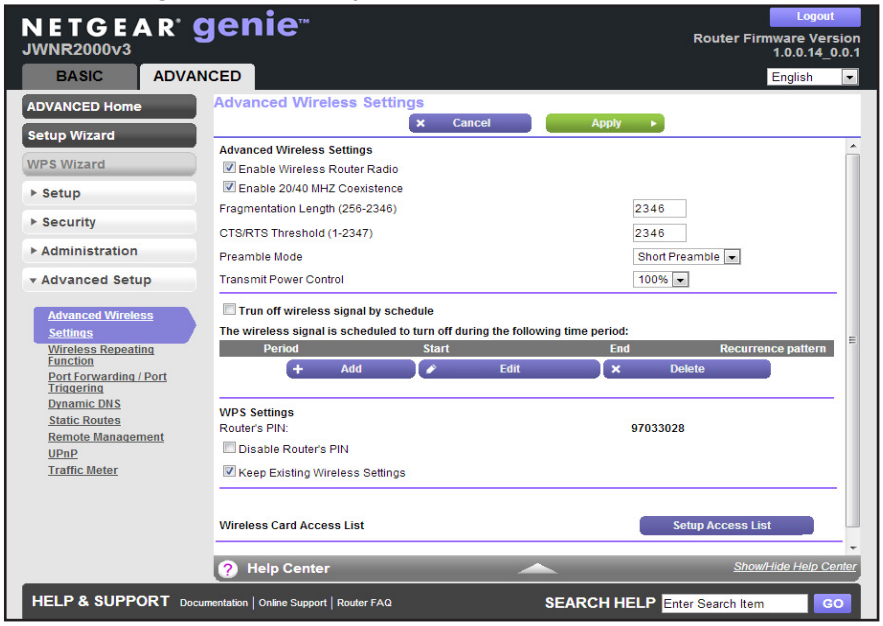
Control the Wireless Radio

By default, the wireless radio is enabled so that you can connect wirelessly to the modem router. You can turn the wireless radio on or off in the Advanced Wireless Settings screen. When the wireless radio is off, you can still use an Ethernet cable for a LAN connection to the modem router.

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

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

   The following screen displays:



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

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

   If you clear this check box, this turns off the WiFi feature of the wireless modem router.

3. Click **Apply**.

   Your changes take effect.

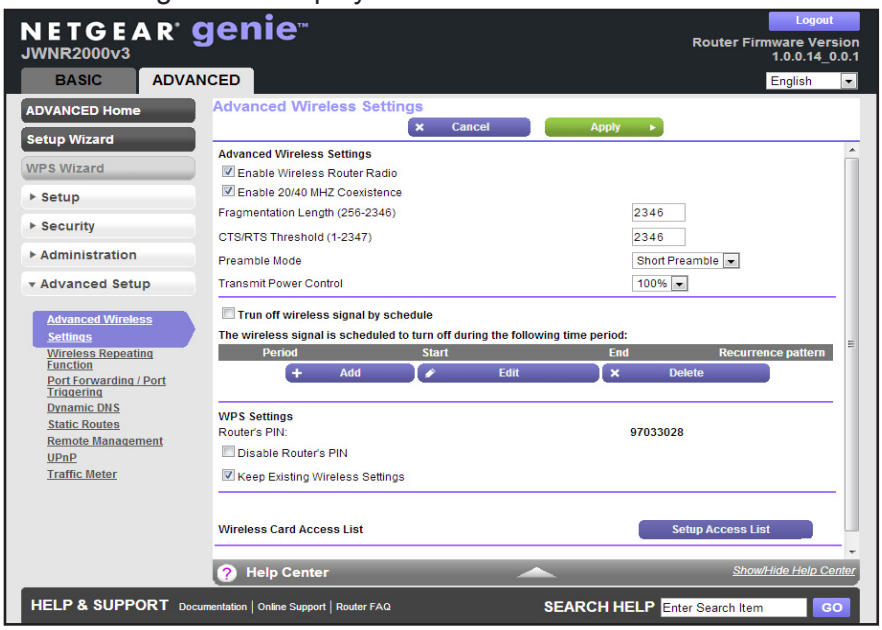
Control Wireless Interference

By default, the 20/40 MHZ Coexistence is enabled so that your wireless network does not interfere with other wireless networks in your area. This setting might reduce the maximum speed of your 2.4 GHz wireless network to half when another wireless network is detected in your environment.

➢ **To turn the 20/40 MHZ Coexistence on or off:**

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

   The following screen displays:



   By default, the Enable 20/40 MHZ Coexistence check box is selected.

2. Select or clear the **Enable 20/40 MHZ Coexistence** check box.

   If you clear this check box, you can maintain maximum speed for your wireless network regardless of other networks in your area.

3. Click **Apply**.

   Your changes take effect.

Control Power Transmission

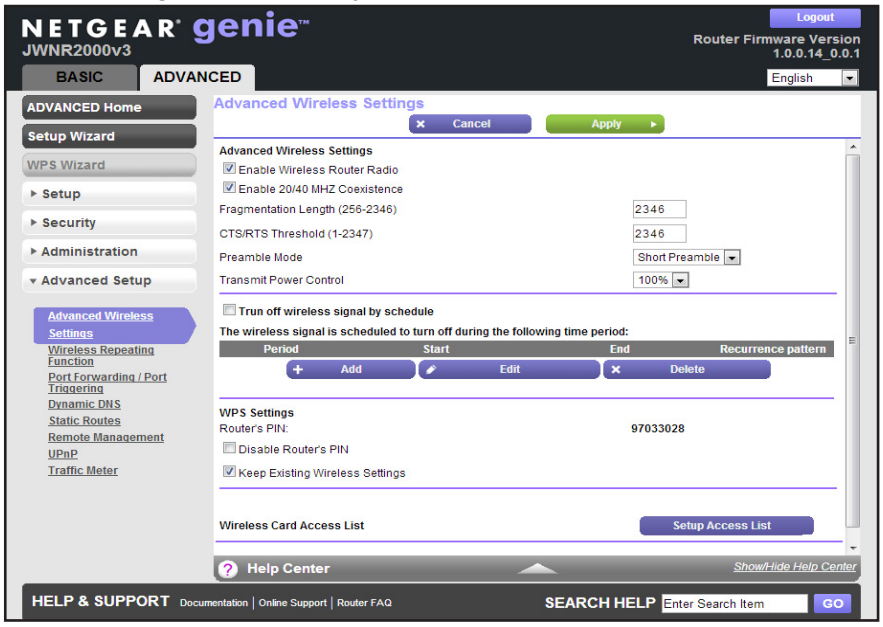
Transmission power control limits the maximum power used when the router transmits packets. The options are 100%, 75%, 50%, and 25%. You can easily turn down the transmission power to ensure that you are utilizing the optimum power that gives you the optimum range while saving money and the environment.

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.

➢ **To configure the transmission power control:**

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

   The following screen displays:



2. In the Transmit Power Control drop-down menu, select the transmission power.
3. Click **Apply**.

   Your changes take effect.

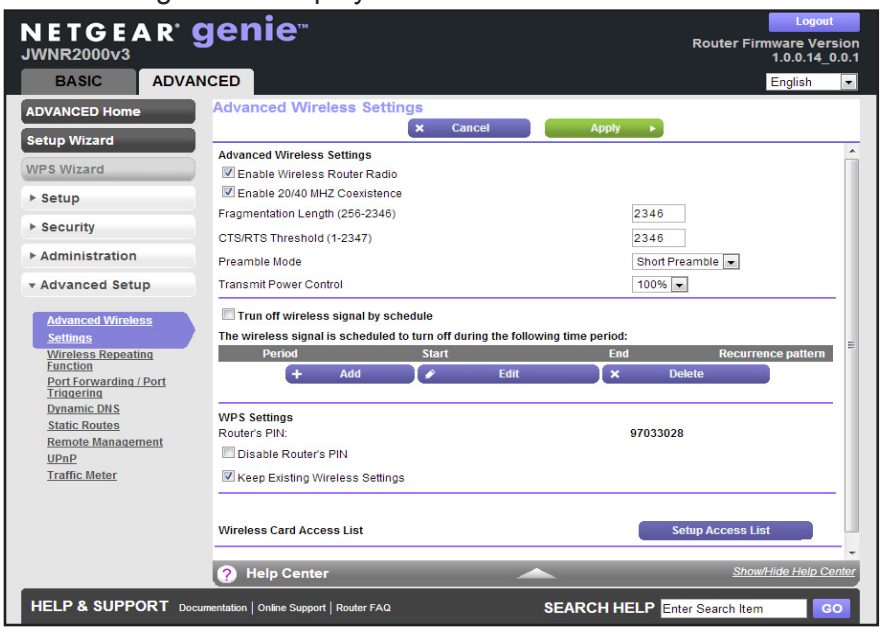
Set Up a Wireless Schedule

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

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

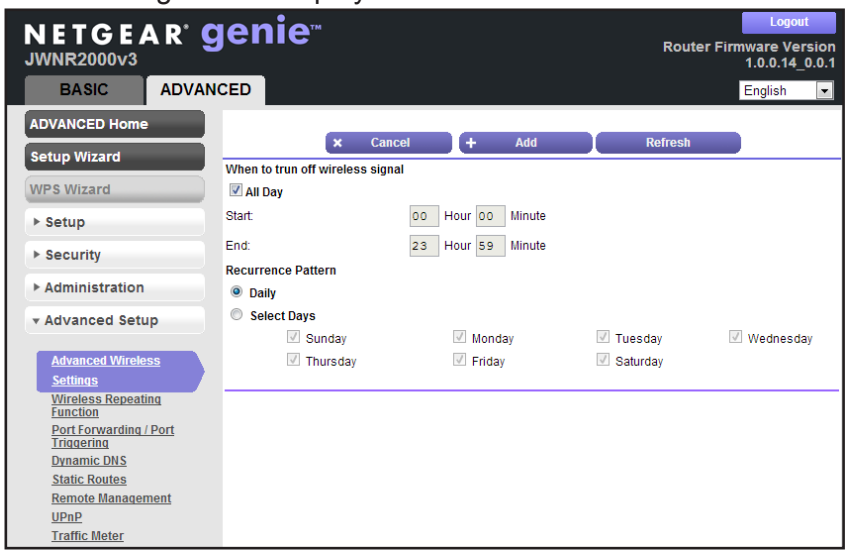
1. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.

The following screen displays:



2. Click **Add**.

The following screen displays:



3. Use the radio buttons and check boxes to set up a period during which you want the wireless signal to be turned off.
4. Click **Apply**.

   The Advanced Wireless Settings screen displays.
5. Select the **Turn off wireless signal by schedule** check box to activate the schedule.
6. Click **Apply**.

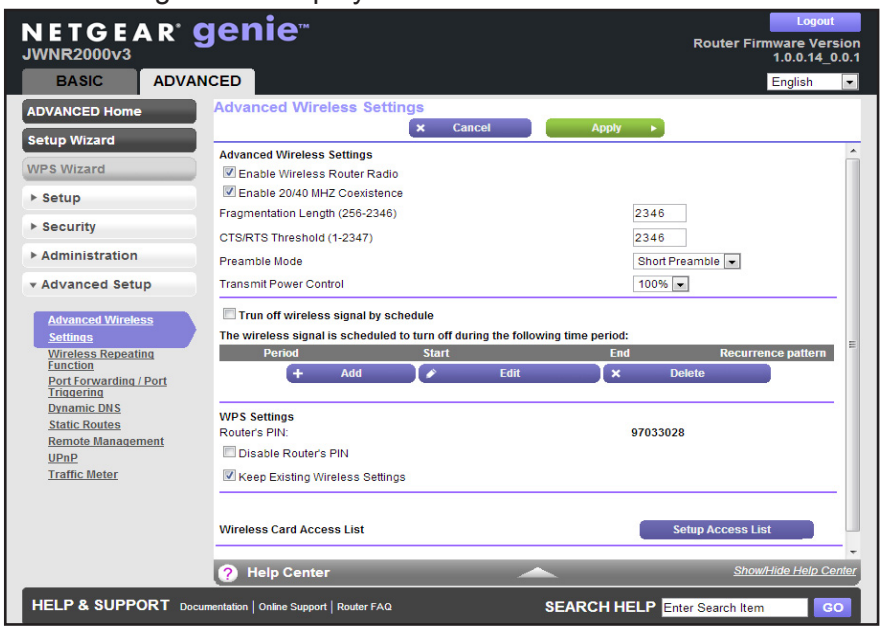
View or Change WPS Settings

You can view or change the WPS settings in the Advanced Wireless Settings screen.

➢ **To specify WPS settings:**

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

   The following screen displays:



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

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

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

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

   By default this check box is selected so that when WPS is used to join the wireless network, the router wireless settings do not change. NETGEAR recommends that you leave this check box selected.

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

4. Click **Apply**.

   Your changes take effect.

Restrict Wireless Access by MAC Address

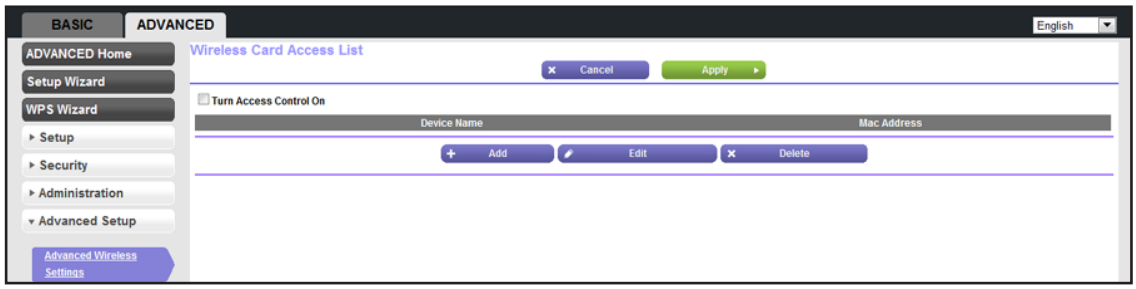
You can set up a list of computers and wireless devices that are allowed to join the wireless network. This list is based on the unique MAC address of each computer and device.

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

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

1. Select **ADVANCED > Advanced Setup > Advanced Wireless Settings**.
2. Click **Setup Access List**.

   The Wireless Card Access List screen displays.



3. Click **Add** to add a wireless device to the wireless access control list.

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

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

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

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

5. Click **Add** to add this wireless device to the Wireless Card Access List.

   The screen changes back to the Wireless Card Access List screen.

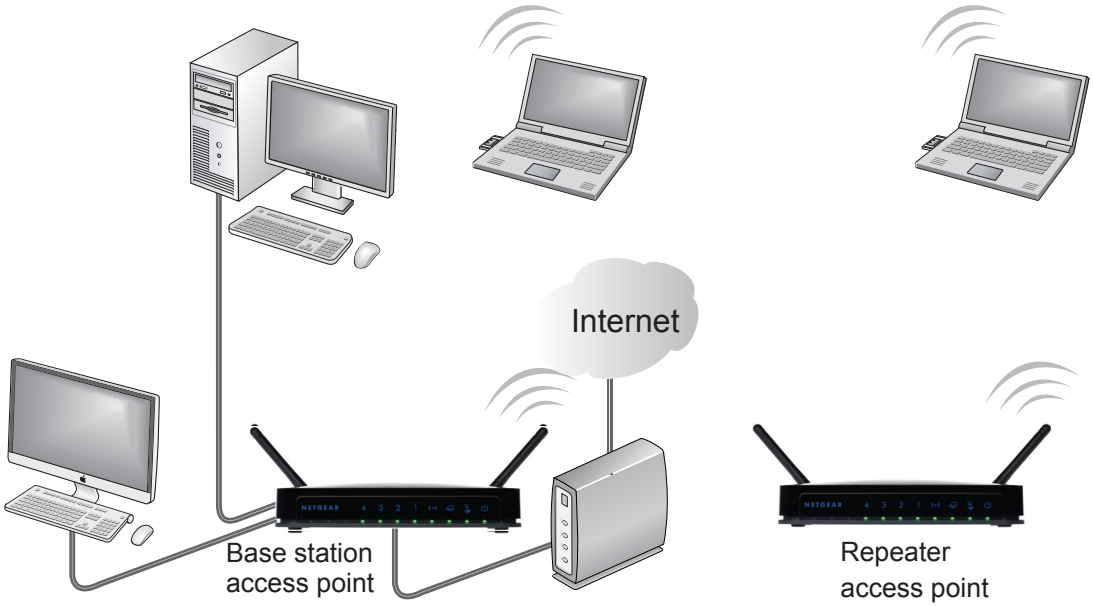
6. Add each computer or device that you want to allow to connect wirelessly.
7. Select the **Turn Access Control On** check box.
8. Click **Apply**.

Wireless Repeating Function

You can configure the router to be used as a wireless access point (AP), which enables it 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.

Note: If you use the wireless repeating function, 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 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.



The scenario includes these components:

- **Wireless base station**. The router acts as the parent access point, bridging traffic to and from the child repeater access point. The base station also handles wireless and wired local computers. To configure this mode, you must know the MAC addresses of the child repeater access point.
- **Wireless repeater**. The router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you must know the MAC address of the remote parent access point.

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

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

- Both access points must use the same SSID, wireless channel, and encryption mode.
- Both access points must be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) must be configured to operate in the same LAN network address range as the access points.

➢ **To view or change the wireless repeater settings for the router:**

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

2. Configure the following wireless repeater settings:
   - **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 check box.
   - **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 the **Disable Wireless Client Association** check box.
- If you want all client traffic to go through the other access point (repeater with wireless client association), leave the Disable Wireless Client Association 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 check box.
- **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.

3. Click **Apply**.

   Your settings are saved.

Set Up the Base Station

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

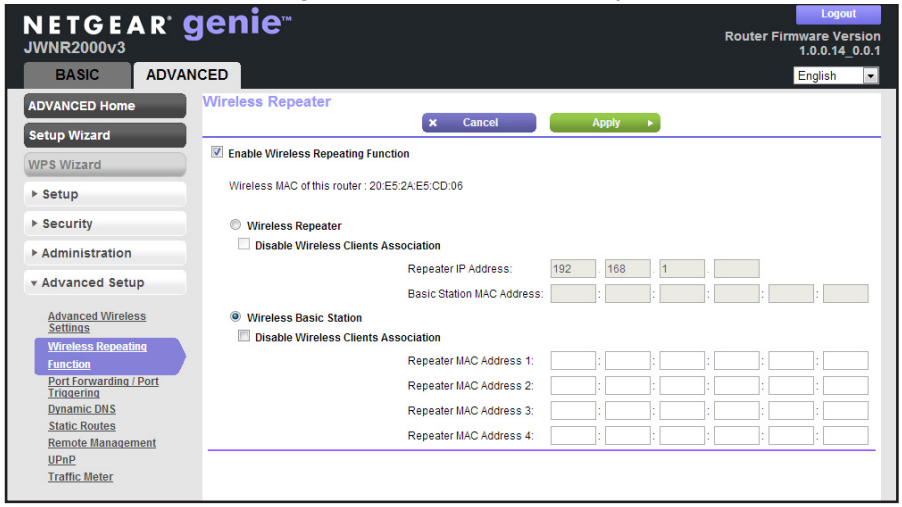
➢ **To set up the base station:**

1. Set up both units with the same wireless settings (SSID, mode, channel, and security).

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

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

   The Wireless Repeating Function screen displays.



3. Select the **Enable Wireless Repeating Function** check box.
4. Select the **Wireless Base Station** radio button.
5. Enter the MAC address for one or more repeater units.
6. Click **Apply**.

   Your changes are saved.

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 JWNR2000v3 base station with a non-NETGEAR router as the repeater, you might need to change additional 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 will be the repeater.
2. Select **BASIC > Wireless Settings** and verify that the wireless settings match the base unit exactly.

   The wireless security option must be set to **None** or **WEP**.
3. Select **ADVANCED > Advanced Setup > Wireless Repeating Function**.
4. Select the **Enable Wireless Repeating Function** check box.
5. Select the **Wireless Repeater** radio button.
6. Complete the Repeater IP Address field.

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

   Your changes are saved.
8. 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 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 your router does not recognize their replies.

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

Remote Computer Access Basics

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

The following 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:
   - **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.

   The request message is sent to your router.
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 step 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 assigned by the router, such as 33333. This step 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.
   - **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.

   The web server then sends this reply message to your router.
5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message to restore the original address information that was 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. 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 additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule that you 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 there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113 associated with your computer. The router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

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

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 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 NAT on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

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

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

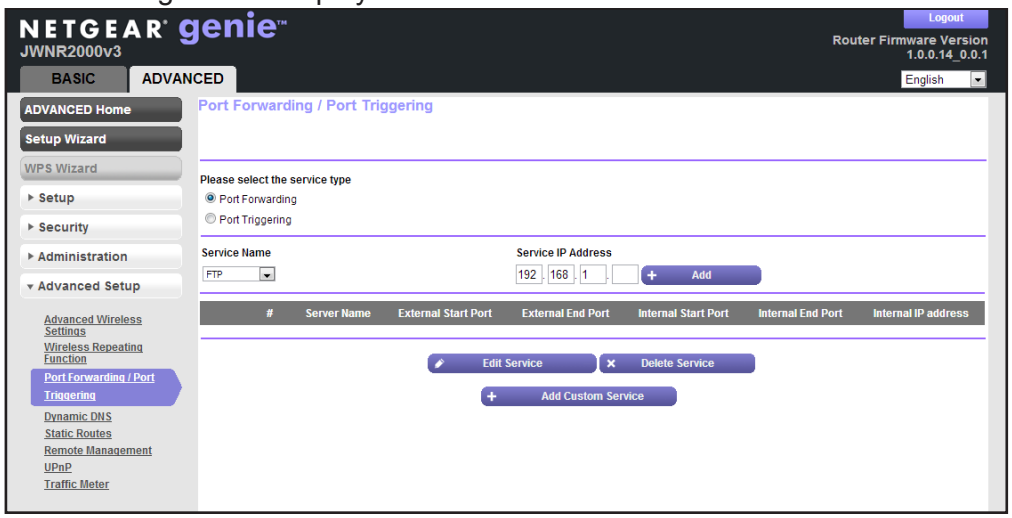
Before starting, determine which type of service, application, or game you want to provide. Find out the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your JWNR2000v3 router.

➢ **To set up port forwarding:**

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

   The following screen displays:



   Port Forwarding is selected as the service type.

2. From the Service Name drop-down menu, select the service or game that you will host on your network.

   If the service does not appear in the menu, see *Add a Custom Service* on page 87.

3. In the Service IP Address field, enter the last digit of the IP address of your local computer that will provide this service.
4. Click **Add**.

   The service appears in the list on the screen.

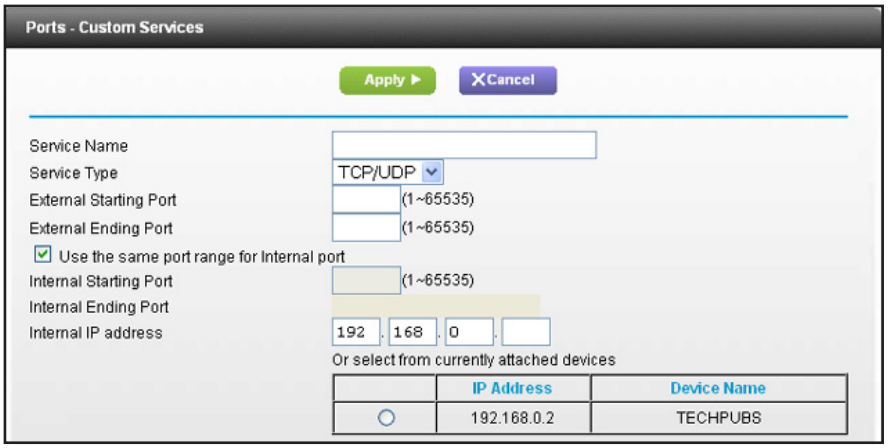
Add a Custom Service

To define a service, game, or application that does not appear in the Service Name drop-down menu, first determine which port number or range of numbers the application uses. You can usually get this information by contacting the publisher of the application or user groups or newsgroups.

➢ **To add a custom service:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.
3. Click the **Add Custom Service** button.

   The following screen displays:



4. In the Service Name field, enter a descriptive name.
5. From the Service Type drop-down menu, select the protocol.

   If you are unsure, select **TCP/UDP**.
6. In the External Starting Port field, enter the beginning port number.
   - If the service uses only one port, enter the port number in the External Ending Port field.
   - If the service uses a range of ports, enter the end port number in the External Ending Port field.
7. In the Internal Starting Port field, enter the beginning port number.
   - If the service uses only one port, enter the port number in the Internal Ending Port field.
   - If the service uses a range of ports, enter the end port number in the Internal Ending Port field.
8. In the Internal IP Address field, enter the IP address of your local computer that will provide this service, or select the radio button next to an IP address from the currently attached devices.
9. 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. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.
3. Select the radio button next to the service name in the list.
4. 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.

   For more information, see *Dynamic DNS* on page 90.

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

Set Up Port Triggering

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

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

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

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

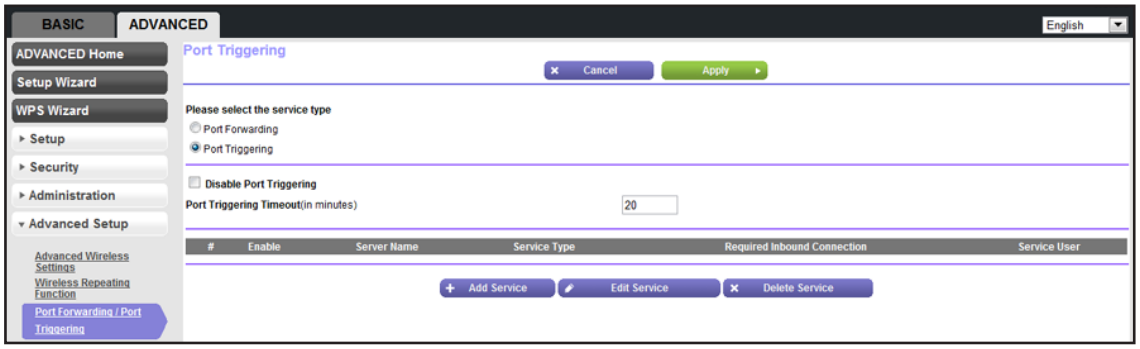
Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 94.

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

➢ **To set up port triggering:**

1. Select **ADVANCED > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button.

   The Port Triggering screen displays:



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

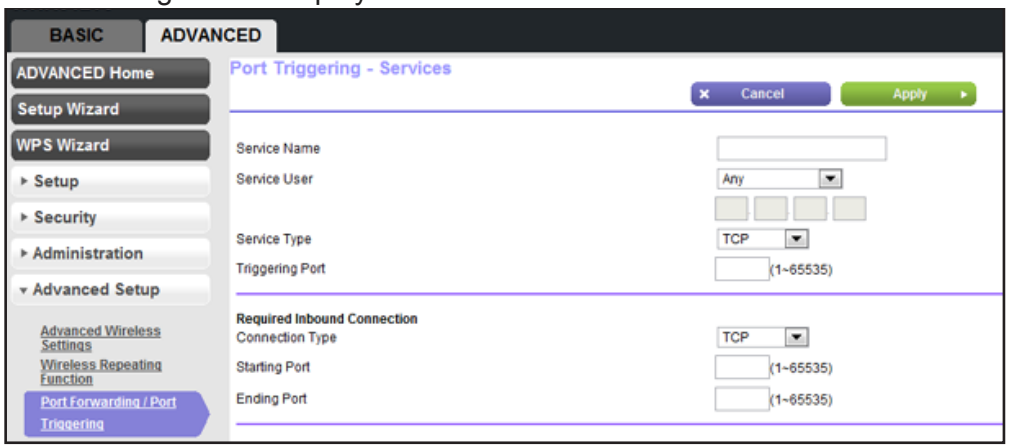
   Note: *If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.*

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**.

The following screen displays:



6. In the Service Name field, type a descriptive service name.
7. From the Service User drop-down menu, select **Any** (the default) to allow any computer on the Internet to use this service.

   Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.
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 will cause the inbound ports to be opened.
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 list on the Port Triggering screen.

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 will be, 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.

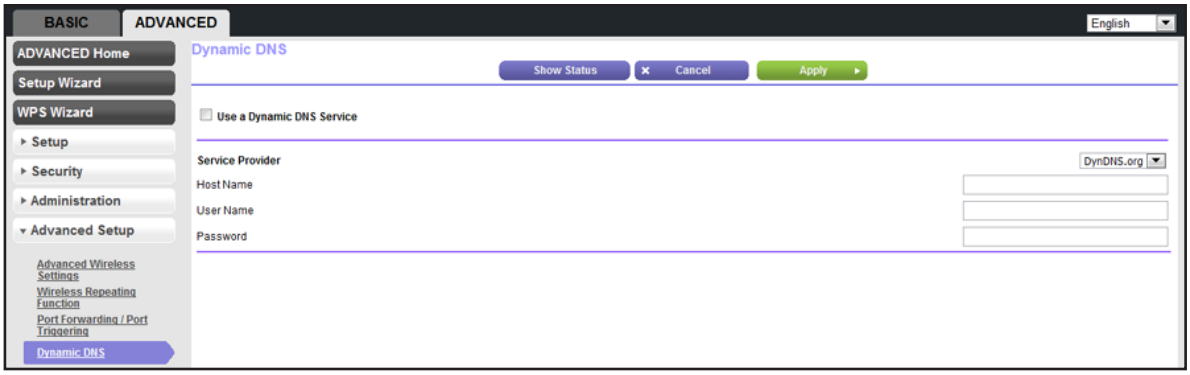
Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit *http://www.dyndns.org* and obtain an account and host name that you configure in the router. Then, whenever your ISP-assigned IP address changes, your router

automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at http://hostname.dyndns.org.

➢ **To set up Dynamic DNS:**

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

   The following screen displays:



2. Register for an account with one of the Dynamic DNS service providers whose names appear in the Service Provider drop-down menu.
3. Select the **Use a Dynamic DNS Service** check box.
4. Select the URL of your Dynamic DNS service provider from the Service Provider drop-down menu.
5. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
6. Type the user name for your Dynamic DNS account.

   Enter the name that you use to log in to your account, not your host name.

7. Type the password (or key) for your Dynamic DNS account.
8. Click **Apply.**

   Your configuration is saved.

Static Routes

Static routes provide additional routing information to your router. Typically, you do not need to add static routes. You 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 be denied by the company's firewall.

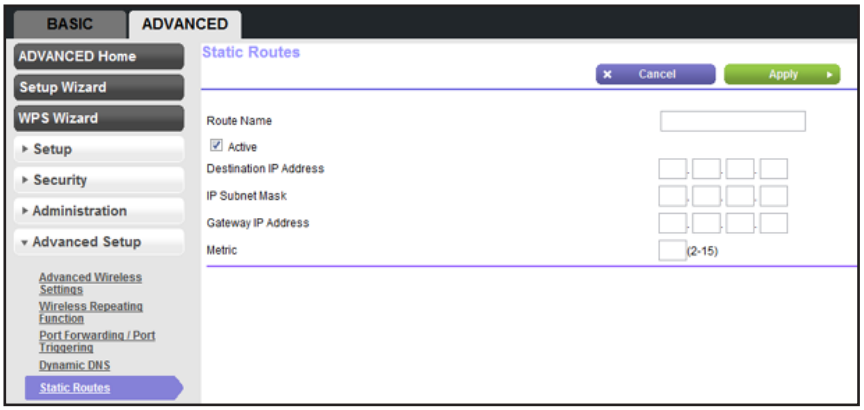
In this case, you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. In this example:

- 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 will work because the ISDN router is on the LAN.

➢ **To set up a static route:**

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

   The following screen displays:



3. In the Route Name field, type a name for this static route (for identification purposes only).
4. Select the **Active** check box to make this route effective.
5. Type the IP address of the final destination.
6. Type the IP subnet mask for this destination.

   If the destination is a single host, type **255.255.255.255**.

7. Type the gateway IP address.

   The gateway IP address must be a router on the same LAN segment as the JWNR2000v3 router.

8. 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 you have a direct connection, set it to 1.

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

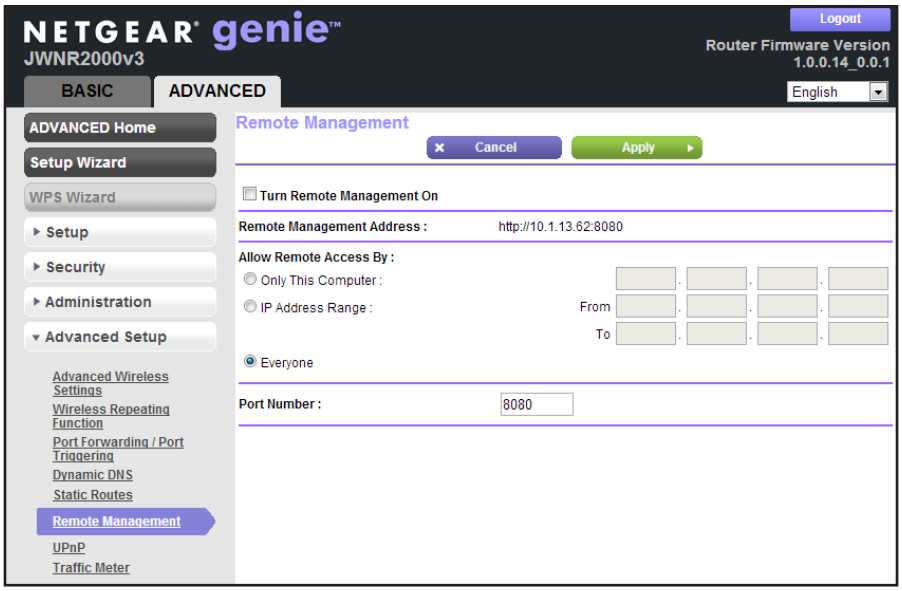
Remote Management

The remote management feature lets you upgrade or check the status of your JWNR2000v3 router over the Internet.

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

➢ **To set up remote management:**

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



2. Select the **Turn Remote Management On** check box.
3. In the Allow Remote Access By section, specify the external IP addresses to be allowed to access the router's remote management, as follows:
   - To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.
   - To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.
   - To allow access from any IP address on the Internet, select **Everyone**.

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

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

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

5. Click **Apply**.

   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

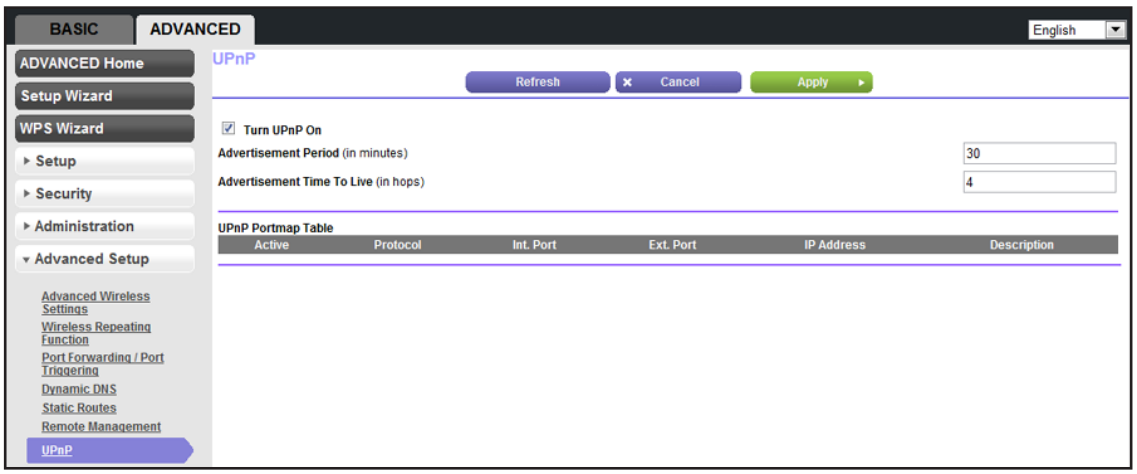
Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

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

➢ **To enable Universal Plug and Play:**

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

   The UPnP screen displays.



2. Configure the UPnP settings, as follows:
   - **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 additional 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 four hops. The default value is fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.
- **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently 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**

   Your settings are saved.

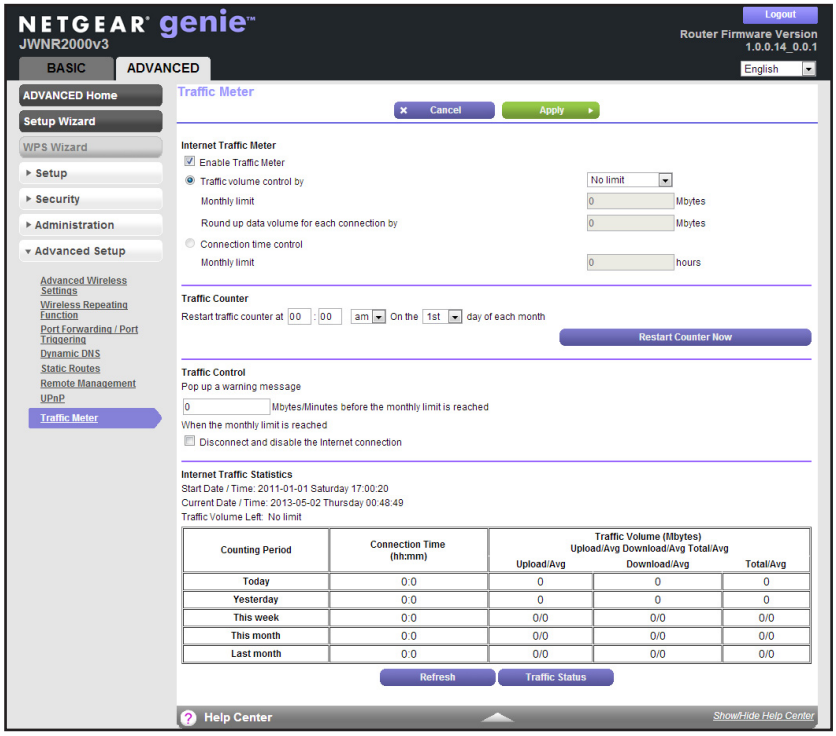
Traffic Meter

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 Setup > Traffic Meter**.

The following screen displays:



2. To enable the traffic meter, select the **Enable Traffic Meter** check box.
3. 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. To limit the amount of data traffic allowed per month, specify how many Mbytes per month are allowed or specify 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.
   - 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 about Internet traffic status on your router.
9. Click **Apply**.

   Your settings are saved.

Troubleshooting

8

This chapter provides information to help you diagnose and solve problems you might have with your router. If you do not find the solution here, visit the NETGEAR support site at *http://support.netgear.com* for product and contact information.

This chapter contains the following sections:

Quick Tips

This section describes tips for troubleshooting some common problems.

Sequence to Restart Your Network

Be sure to restart your network in this sequence:

1. Turn off *and* unplug the modem.
2. Turn off the router and computers.
3. Plug in the modem and turn it on. Wait two minutes.
4. Turn on the router and wait two minutes.
5. Turn on the computers.

Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in.

The Internet LED on the router is on if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.

For each powered-on computer connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED is lit.

Wireless Settings

Make sure that the wireless settings in the computer and router match exactly.

For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer must match exactly.

If you set up an access list in the Advanced Wireless Settings screen, you must add each wireless computer's MAC address to the router's access list.

Network Settings

Make sure that the network settings of the computer are correct.

Wired and wirelessly connected computers must have network (IP) addresses on the same network as the router. The simplest method is to configure each computer to obtain an IP address automatically using DHCP.

Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen.

Troubleshoot with the LEDs

After you turn on power to the router, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is lit.
2. After approximately 30 seconds, verify the following:
   - The Power LED is solid green.
   - The Internet LED is lit.
   - A numbered LAN port LED is lit for any local port that is connected to a computer. A lit LAN port LED indicates that a link has been established to the connected device.

The LEDs on the front panel of the router can be used for troubleshooting.

Power LED Is Off

Check the following:

- Make sure that the power cord is securely connected to your router and that the power adapter is securely connected to a functioning power outlet.
- Check that you are using the 5 VDC, 1A power adapter that NETGEAR supplied for this product.

If the error persists, you have a firmware or hardware problem. For recovery instructions or help with a hardware problem, contact technical support at *www.netgear.com/support.*

Internet or LAN Port LEDs Are Off

If either the Internet LED or the LAN port LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the modem or computer.
- Make sure that power is turned on to the connected modem or computer.
- Be sure that you are using the correct cable:

  When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Wireless LED Is Off

If the Wireless LED stays off, use NETGEAR genie to turn on the wireless radio. For more information, see *Advanced Wireless Settings* on page 72. The Wireless LED is lit when the wireless radio is turned on.

Cannot Log In to the Router

If you are unable to log in to the router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in an earlier section.
- Make sure that your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254.
- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. Restoring the factory default configuration sets the router's IP address to 192.168.1.1. For more information, see *Factory Settings* on page 108.
- 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 you enter this information.
- If you are attempting to set up your NETGEAR router as an additional router behind an existing router in your network, consider replacing the existing router. NETGEAR does not support such a configuration.
- If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services. For example, the router cannot convert ADSL or cable data into Ethernet networking information. NETGEAR does not support such a configuration.

Cannot Access the Internet

If you can access your router but not the Internet, check to see if the router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful using the Router Status screen.

➢ **To check the WAN IP address:**

1. Start your browser, and select an external site such as *www.netgear.com*.
2. Access the router interface at **www.routerlogin.net.**
3. Select **Administration > Router Status**.
4. Check that an IP address is shown for the Internet port.

   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

Your Router Cannot Obtain an IP Address from the ISP

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network (see *Sequence to Restart Your Network* on page 98).

If your router is still unable to obtain an IP address from the ISP, the problem might be one of the following:

- Your Internet service provider (ISP) might require a login program.

  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.

- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name.

  Assign the computer host name of your ISP account as the account name in the Basic Settings screen.

- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  - Configure your router to clone your computer's MAC address.

Your Router Can Obtain an IP Address from the ISP

If your router can obtain an IP address but your computer is unable to load any web pages from the Internet, the problem might be one of the following:

- Your computer might not recognize any DNS server addresses.

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

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

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

- You might be running login software that is no longer needed.

  If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**.

Troubleshoot PPPoE

If you are using PPPoE, try troubleshooting your Internet connection.

➢ **To troubleshoot a PPPoE connection:**

1. Log in to the router.
2. Select **ADVANCED > Administration > Router Status**.
3. Click **Connection Status**.
4. Check to see if your PPPoE connection is up and working.

   If any of the steps indicate Failed, you can attempt to reconnect by clicking **Renew**. The router continues to attempt to connect indefinitely.

   If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

Note: Unless you connect manually, the router does not authenticate using PPPoE until data is transmitted to the network.

Troubleshoot Internet Browsing

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

- Your computer might not recognize any DNS server addresses. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses.

Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, restart your computer.

Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

- Your computer might not have the router configured as its default gateway.

  Reboot the computer and verify that your computer lists the router address (www.routerlogin.net) as the default gateway address.

- You might be running login software that is no longer needed. If your ISP provided a program to log you in to the Internet (such as WinPoET), you no longer need to run that software after installing your router. You might need to go to Internet Explorer and select **Tools > Internet Options**, click the **Connections** tab, and select **Never dial a connection**.

Changes Not Saved

If the router does not save the changes you make in the router interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser's cache.

Wireless Connectivity

If you are having trouble connecting wirelessly to the router, try to isolate the problem, as follows:

- Does the wireless device or computer that you are using find your wireless network?

  If not, check the Wireless LED on the front of the router. It should be lit. If it is not, you can use the NETGEAR genie to turn the router's wireless radio back on (see *Advanced Wireless Settings* on page 72).

  If you disabled the router's SSID broadcast, then your wireless network is hidden and does not show up in your wireless client's scanning list. By default, SSID broadcast is enabled.

- Does your wireless device support the security that you are using for your wireless network (WPA or WPA2)?
- If you want to view the wireless settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router, and select **Wireless** (see *Basic Wireless Settings* on page 26).

  Note: *Be sure to click **Apply** to save your changes.*

If your wireless device finds your network, but the signal strength is weak, check these conditions:

- Is your router too far from your computer, or too close? Place your computer near the router, but at least 6 feet (1.8 meters) away, and see whether the signal strength improves.
- Are objects between the router and your computer blocking your wireless signal?

Restore the Factory Settings and Password

You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see *Erase the Current Configuration Settings* on page 68).
- Use the Reset button on the back of the router. See *Factory Settings* on page 108. If you restore the factory settings and the router fails to restart, the unit might be defective. If the error persists, you might have a hardware problem and should contact technical support at *http://www.netgear.com/support*.

Troubleshoot Your Network Using the Ping Utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a network by using the ping utility in your computer or workstation.

Test the LAN Path to Your Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

➢ **To ping the router from a Windows computer:**

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 www.routerlogin.net

3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address > with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

If the path is not functioning correctly, you might have one of the following problems:

- Wrong physical connections

  For a wired connection, make sure that the numbered LAN port LED is lit for the port to which you are connected.

  Check that the appropriate LEDs are lit for your network devices. If your router and computer are connected to a separate Ethernet switch, make sure that the link LEDs are lit for the switch ports that are connected to your computer and router.

- Wrong network configuration

  Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

  Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

➢ **To test the path from a Windows computer:**

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the Windows Run window, type the following:

   `ping -n 10` <*IP address*>

   <IP address> is the IP address of a remote device such as your ISP's DNS server.

   If the path is functioning correctly, replies like the ones shown in the previous section are displayed.

   If you do not receive replies, check the following:

   - Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
   - Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
   - Check that your cable or DSL modem is connected and functioning.
   - If your ISP assigned a host name to your computer, enter that host name as the account name in the Basic Settings screen.
   - Your ISP might be rejecting the Ethernet MAC addresses of all but one of your computers.

   Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem. Some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, configure your router to clone or spoof the MAC address from the authorized computer.

Supplemental Information

This appendix provides factory default settings and technical specifications for the N300 Wireless Router JWNR2000v3.

Factory Settings

You can return the router to its factory settings. Insert the end of a paper clip or a similar object to press and hold the **Reset** button on the back of the router for at least seven seconds. The router resets and returns to the factory configuration settings shown in the following table.

Table 3. Factory default settings

Feature		Default behavior
Router login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	AutoSensing
Local network (LAN)	LAN IP	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	GMT
	Time zone daylight saving time	Disabled
	Allow a registrar to configure this router	Enabled
	DMZ	Disabled
Wireless	Wireless communication	Enabled
	SSID name	See router label
	Security	WPA2-PSK (AES)
	Broadcast SSID	Enabled
	Transmission speed	Auto[1]
	Country/region	United States in the US; otherwise varies by region
	RF channel	6 until region selected
	Operating mode	Up to 300 Mbps

Table 3. Factory default settings (continued)

Feature		Default behavior
Firewall	Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests)
	Outbound (communications going out to the Internet)	Enabled (all)

1. Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

Table 4. JWNR2000v3 Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Dynamic DNS, and UPnP.
Power adapter AC plug is localized	• 110V–240V, 50/60 Hz, input • All regions (output): 5 VDC @ 1A, output
Dimensions	173.2 x 135.8 x 34 mm (6.82 x 5.35 x 1.34 in.)
Weight	228.3 g (0.5 lb)
Operating temperature	–5° to 45°C (23º to 113ºF)
Operating humidity	95% maximum relative humidity, noncondensing
Electromagnetic emissions	China CCC & SRRC
LAN	10BASE-T or 100BASE-Tx, RJ-45
WAN	10BASE-T or 100BASE-Tx, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for the previous table.
Radio data rates	Auto Rate Sensing
Data encoding standards	IEEE 802.11b/g/n 2.4GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).
Operating frequency range	2.412–2.462 GHz (US) 2.412–2.472 GHz (Europe ETSI)
802.11 security	WPA-PSK, WPA2-PSK, and WPA/WPA2

Notification of Compliance

B

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Products bearing the CE marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

For indoor use only. Valid in all EU member states, EFTA states, and Switzerland.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N300 Wireless Router JWNR2000v3 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

TV Tuner (on Selected Models)

Note to CATV System Installer: This reminder is provided to call the CATV system installer’s attention to Section 820-93 of the National Electrical Code, which provides guidelines for proper grounding and, in particular, specifies that the Coaxial cable shield be connected to the grounding system of the building as close to the point of cable entry as possible.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N300 Wireless Router JWNR2000v3) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Interference Reduction Table

The following table shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby monitor - analog	20 feet / 6 meters
Baby monitor - digital	40 feet / 12 meters
Cordless phone - analog	20 feet / 6 meters
Cordless phone - digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Index

O

P

Q

R

S

T