NETGEAR

N600 Wireless Dual Band Router WNDR3400v2

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

November 2016
202-10828-05

Support

Thank you for purchasing this NETGEAR product. You can visit *www.netgear.com/support* to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Conformity

For the current EU Declaration of Conformity, visit *http://kb.netgear.com/app/answers/detail/a_id/11621*.

Compliance

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

See the regulatory compliance document before connecting the power supply.

Trademarks

© NETGEAR, Inc., NETGEAR and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Contents

Chapter 1 Hardware Setup

Unpack Your Router 8
Position Your Router 8
Prepare the Router 9
Hardware Features 11
Front Panel 11
Back Panel 13
Label 14
Cable Your Router 15
Verify the Cabling 15

Chapter 2 Getting Started with NETGEAR genie

Router Setup Preparation 17
Use Standard TCP/IP Properties for DHCP 17
Gather ISP Information 17
Wireless Devices and Security Settings 17
Types of Logins and Access 17
NETGEAR genie Setup 18
Use NETGEAR genie after Installation 19
Upgrade Router Firmware 19
Router Dashboard (Basic Home Screen) 20
Add Wireless Devices or Computers to Your Network 21
Manual Method 21
Wi-Fi Protected Setup (WPS) Method 21

Chapter 3 genie Basic Settings

Internet Setup 23
Internet Setup Screen Fields 23
Attached Devices 25
Parental Controls 26
ReadySHARE USB Storage 26
Basic Wireless Settings 27
Wireless Setup Screen Fields 29
Change WPA Security Option and Passphrase 30
Guest Networks 31
Guest Network Wireless Security Options 32

Chapter 4 genie Advanced Home

Setup Wizard 35
WPS Wizard 36
Setup Menu 37
WAN Setup 38
Default DMZ Server 39
Change the MTU Size 39
LAN Setup 41
LAN Setup Screen Settings 42
Use the Router as a DHCP Server 42
Address Reservation 43
Quality of Service (QoS) Setup 44

Chapter 5 USB Storage

USB Drive Requirements 50
ReadySHARE Access 50
File-Sharing Scenarios 51
Basic Settings 52
Add or Edit a Network Folder 53
USB Storage Advanced Settings 54
Safely Remove a USB Drive 56
Specify Approved USB Devices 56
Connect to the USB Drive from a Remote Computer 57
Access the Router's USB Drive Remotely Using FTP 57

Chapter 6 Security

Keyword Blocking of HTTP Traffic 60
Block Services (Port Filtering) 61
Schedule Blocking 62
Security Event Email Notifications 63

Chapter 7 Administration

Upgrade the Router Firmware 66
View Router Status 67
Router Information 67
Internet Provider (WAN) Setup 67
Wireless Settings (2.4 GHz and 5 GHz) 70
Guest Network (2.4 GHz and 5 GHz) 71
View Logs of Web Access or Attempted Web Access 71
Manage the Configuration File 72
Backup Settings 73
Restore Configuration Settings 73
Erase 73
Set Password 74
Password Recovery 74

Chapter 8 Advanced Settings

Advanced Wireless Settings 77
Wireless Repeating Function (WDS) 78
Wireless Repeating Function 79
Set up the Base Station 80
Set up a Repeater Unit 81
Port Forwarding and Triggering 82
Remote Computer Access Basics 82
Port Triggering to Open Incoming Ports 83
Port Forwarding to Permit External Host Communications 84
How Port Forwarding Differs from Port Triggering 85
Set up Port Forwarding to Local Servers 86
Add a Custom Service 87
Editing or Deleting a Port Forwarding Entry 88
Set up Port Triggering 89
Dynamic DNS 91
Static Routes 93
Remote Management 95
USB Settings 96
Universal Plug and Play 96
IPv6 98
Traffic Meter 98

Chapter 9 Troubleshooting

Quick Tips 101
Sequence to Restart Your Network 101
Check Ethernet Cable Connections 101
Wireless Settings 101
Network Settings 101
Troubleshooting with the LEDs 102
Power/Test LED Is Off or Blinking 102
Power/Test LED Stays Amber 102
LEDs Never Turn Off 102
Internet or Ethernet Port LEDs Are Off 103
Wireless LEDs Are Off 103
The Push 'N' Connect (WPS) Button Blinks Amber 103
Cannot Log in to the Router 103
Cannot Access the Internet 104
Troubleshooting PPPoE 105
Troubleshooting Internet Browsing 106
Changes Not Saved 106
Incorrect Date or Time 107
Wireless Connectivity 107
Wireless Signal Strength 107
Restore the Factory Settings and Password 108
Troubleshoot Your Network Using the Ping Utility 108
Test the LAN Path to Your Router 108

Test the Path from Your Computer to a Remote Device 109

Appendix A Supplemental Information

Factory Settings 110
Technical Specifications 112

Appendix B Notification of Compliance

Index

Hardware Setup

1

Getting to know your router

The N600 Wireless Dual Band Router WNDR3400v2 provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). It is compatible with all major DSL Internet service providers, lets you block unsafe Internet content and applications, and protects the devices (PCs, gaming consoles, and so on) that you connect to your home network.

Note: 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. *Chapter 3, genie Basic Settings*, explains how to set up your Internet connection.

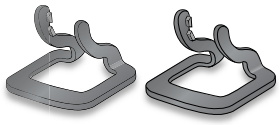
This chapter contains the following sections:

- *Unpack Your Router*
- *Position Your Router*
- *Hardware Features*
- *Cable Your Router*
- *Verify the Cabling*

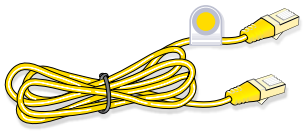
Unpack Your Router

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

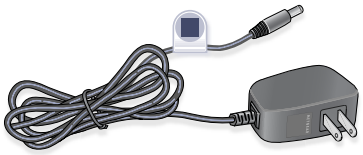
N600 wireless router



Router stand
(two pieces)



Ethernet cable



Power adapter

Your box should contain the following items:

- N600 Wireless Dual Band Router WNDR3400v2
- Router stand (two pieces)
- 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.

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, PCs, 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.

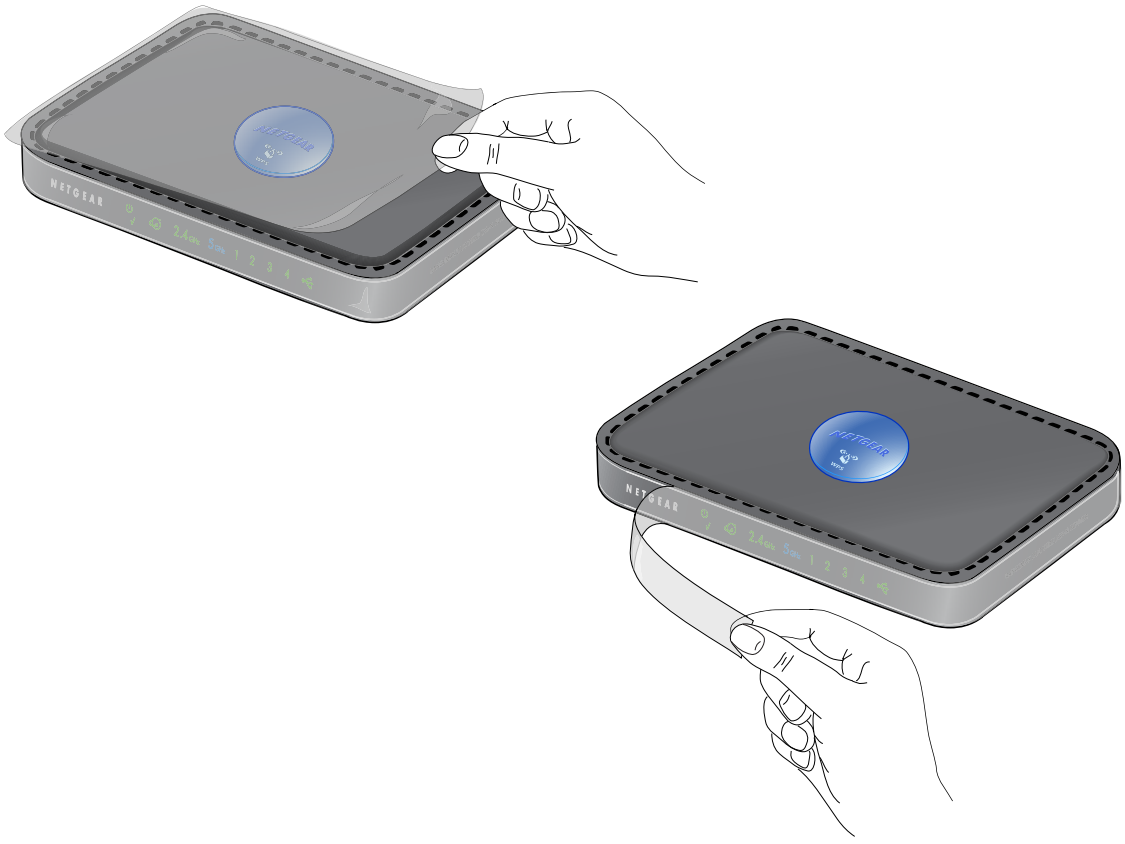
To reduce interference when you use multiple access points, ensure that adjacent access points use different radio frequency channels. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

Prepare the Router

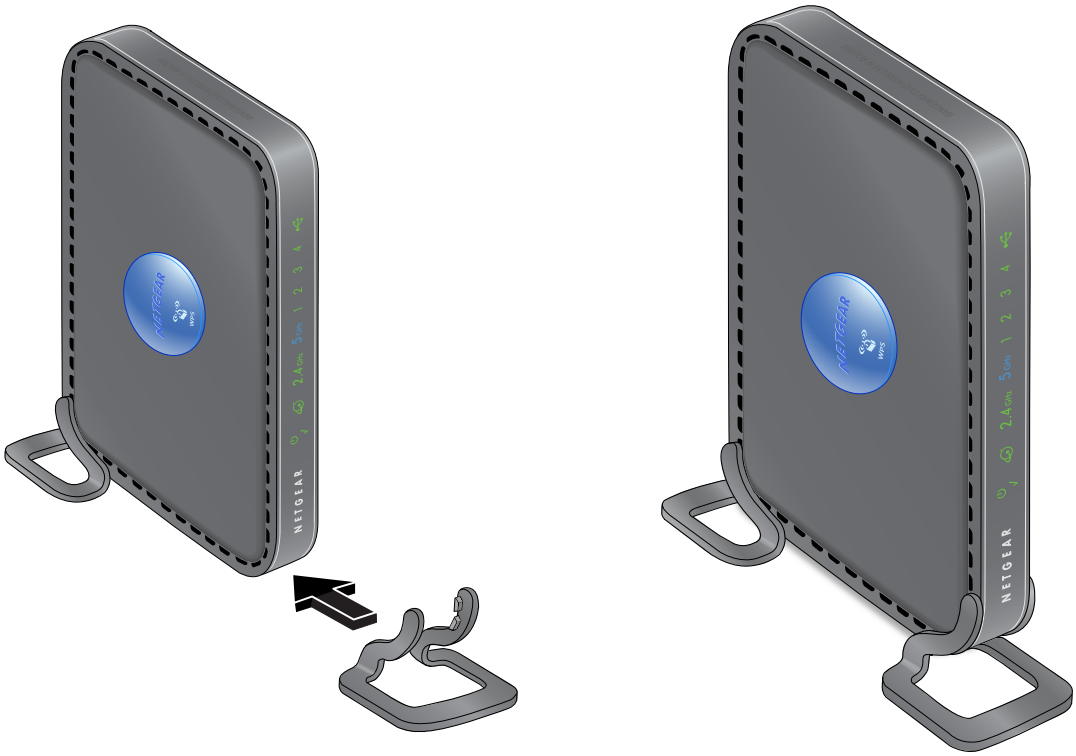
To ensure proper heat dissipation and for router stability, it is important that you connect the stand and place your router in an upright position.

➢ **To prepare your router for installation:**

1. Carefully peel off the protective film covering the top and sides of your router.



2. Set up your N600 Wireless Dual Band Router by inserting the tabs of the stand (supplied with your router) into the slots on the bottom of your router as shown.



3. Place your router in an area suitable for installation (near an AC power outlet and accessible to the Ethernet cables for your wired computers).

Hardware Features

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

Front Panel

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

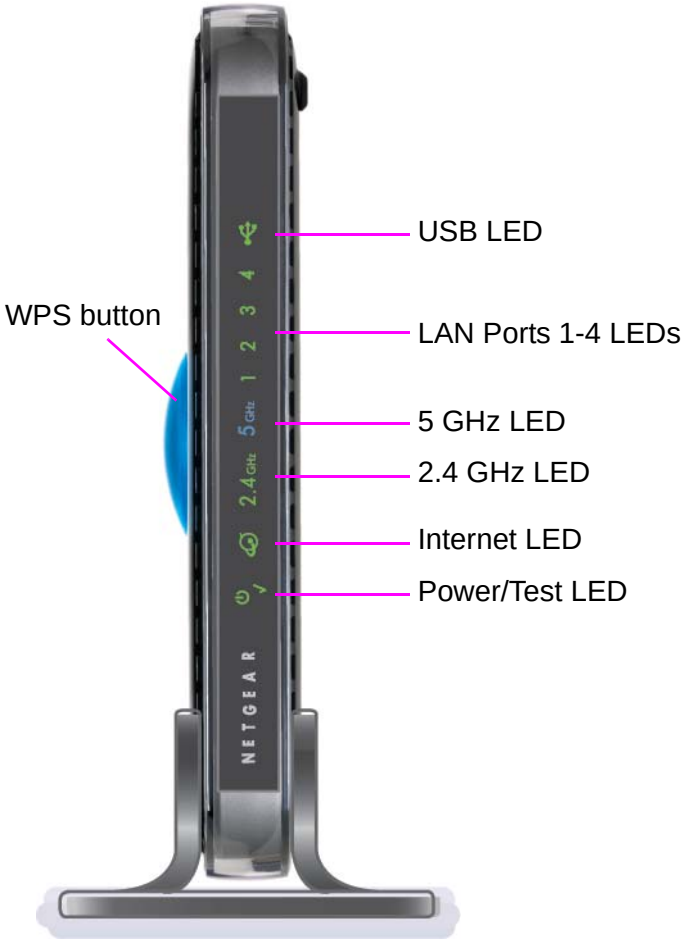


Table 1. Front panel LED descriptions

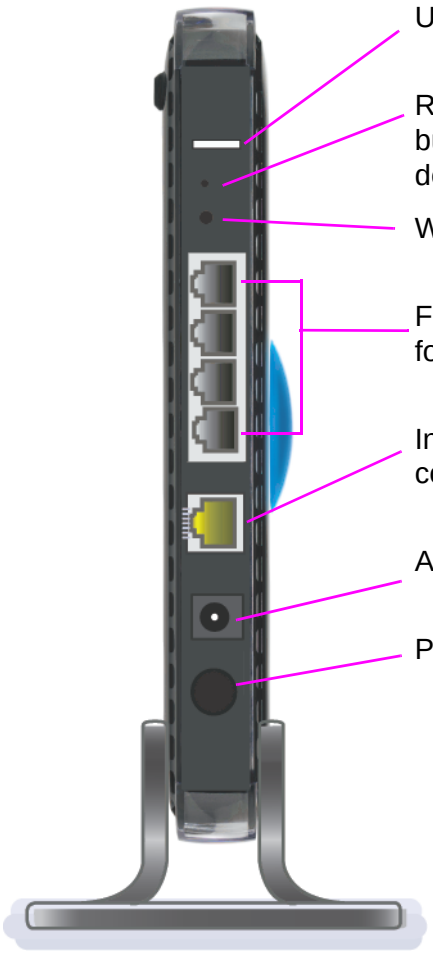
LED	Description
USB	• **Solid green**. The local Ethernet ports have detected wired links with PCs. • **Blinking green**. Data is being transmitted or received. • **Off**. No link is detected on these ports.

Table 1. Front panel LED descriptions (continued)

LED	Description
LAN ports 1–4	• **Solid green**. The LAN port has detected a 100 Mbps link with an attached device. • **Solid amber**. The LAN port has detected a 10 Mbps link with an attached device. • **Off**. No link is detected on this port.
5 GHz	• **Solid blue**. The wireless radio is operating. • **Blinking blue**. Data is being sent or received over the wireless network. • **Off**. The wireless radio is off.
2.4 GHz	• **Solid blue**. The wireless radio is operating. • **Blinking blue**. Data is being sent or received over the wireless network. • **Off**. The wireless radio is off.
Internet	• **Solid amber**. The IP address has not been acquired. • **Solid green**. An IP address was received; ready to transmit data. • **Blinking green**. Data is being sent to or received from the Internet. • **Off**. No Ethernet cable is connected between the router and the modem.
Power/Test	• **Solid amber**. The unit is starting up after being powered on. • **Solid green**. The power is on and the router is ready. • **Blinking amber**. A firmware update is in progress. • **Blinking green**. The firmware is corrupt. • **Off**. Power is not supplied to the router.
WPS	• **Solid green**. Indicates that wireless security is enabled. • **Blinking green**. The router is using WPS to add a wireless device to the network. • **Off**. No WPS connection exists.

Back Panel

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



USB port

Restore Factory Settings button. Press and hold this button for about 5 seconds to reset the router to its factory default settings.

WiFi On/Off button

Four local area network (LAN) 10/100 Mbps Ethernet ports for connecting the router to your local computers.

Internet/Wide Area Network (WAN) Ethernet port for connecting the router to a cable or DSL modem.

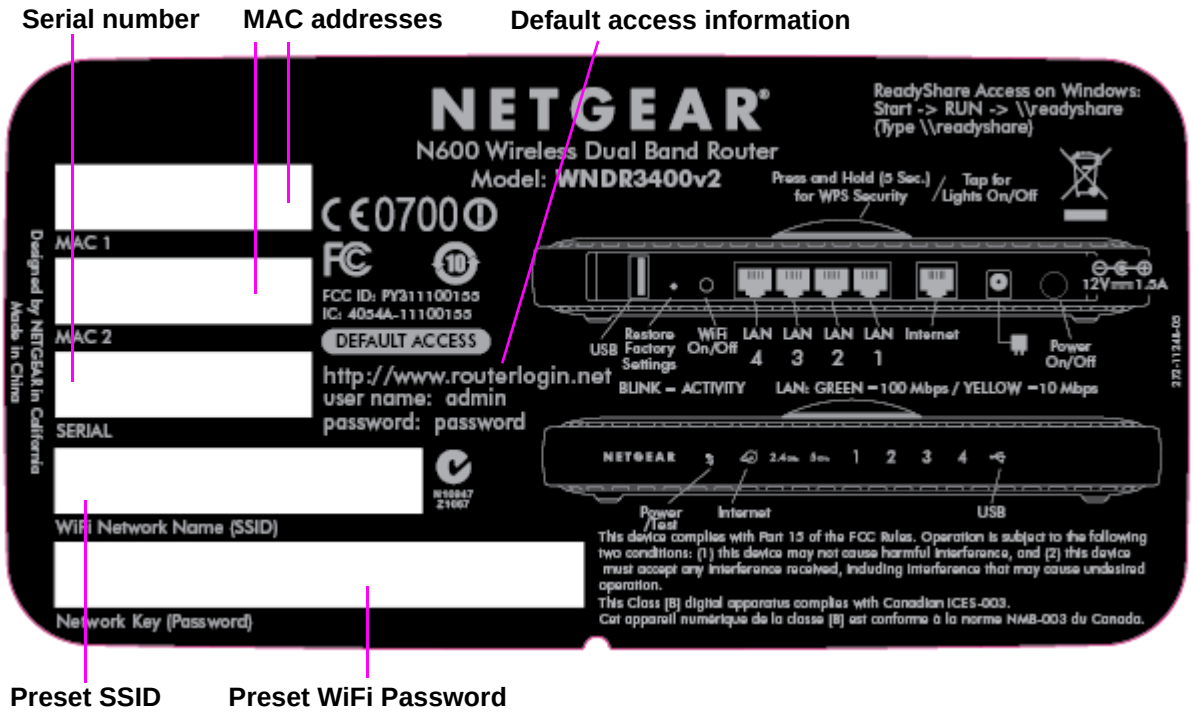
AC power adapter outlet for connecting the power adapter.

Power On/Off button.

See *Factory Settings* on page 110 for information about restoring factory settings.

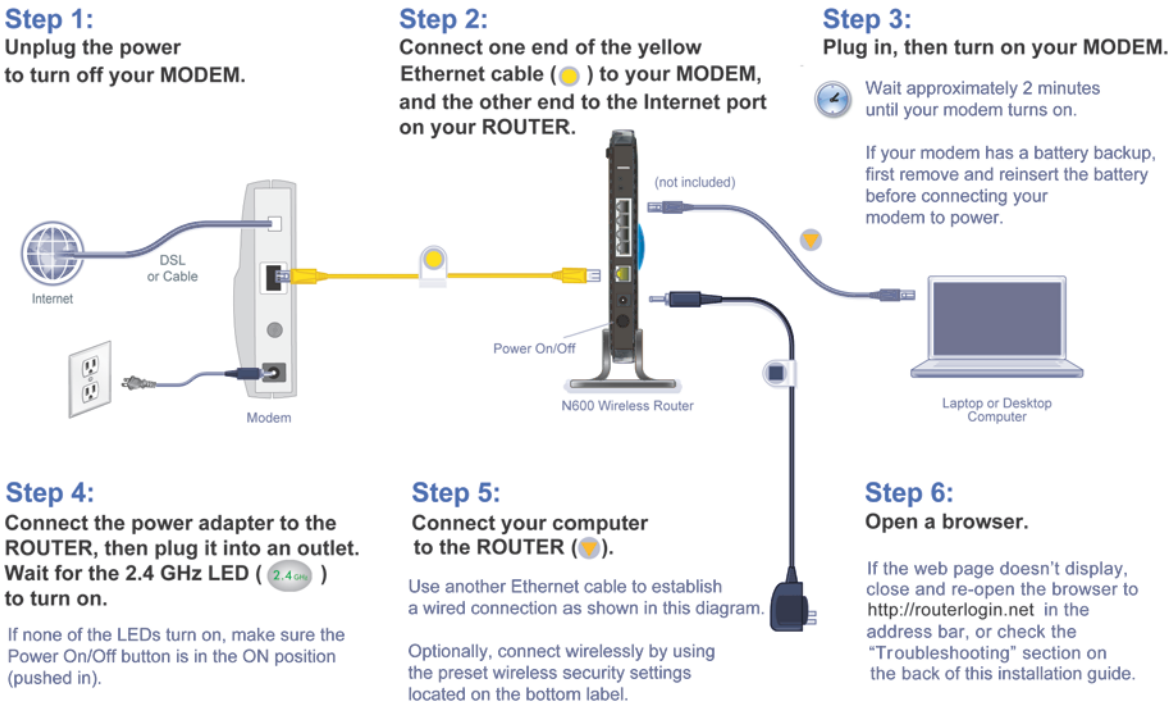
Label

The label on the bottom of the router shows the WPS PIN, login information, MAC address, and serial number.



Cable Your Router

The installation guide that came in the box has a cabling diagram on the first page.



Verify the Cabling

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

- The Power/Test LED is green when the router is turned on.
- The LAN ports are green for each Windows computer cabled to the router by an Ethernet cable.
- The Wireless LEDs are on.
- The Internet LED is lit. If it is not, make sure that the Ethernet cable is securely attached to the router Internet port and the modem, and that the modem is powered on.

Verify that the LAN LEDs (1 through 4) are lit for any computers cabled to the router by an Ethernet cable.

Getting Started with NETGEAR genie

2

Connecting to the router

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

This chapter contains the following sections:

- *Router Setup Preparation*
- *Types of Logins and Access*
- *NETGEAR genie Setup*
- *Use NETGEAR genie after Installation*
- *Upgrade Router Firmware*
- *Router Dashboard (Basic Home Screen)*
- *Add Wireless Devices or Computers to Your Network*

Router Setup Preparation

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

Use Standard TCP/IP Properties for DHCP

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

Gather ISP Information

If you have DSL broadband service, you might need the following information to set up your router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer need to launch the ISP login program on your computer to access the Internet. When you start an Internet application, your router automatically logs you in.

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

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security supported by the router. See *Basic Wireless Settings* on page 27 for information about the router's preconfigured security settings.

Types of Logins and Access

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

- **Router login** logs you in to the router interface from NETGEAR genie. See *Use NETGEAR genie after Installation* on page 19 for details about this login.
- **ISP login** logs you in to your Internet service. Your service provider provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.

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

NETGEAR genie Setup

NETGEAR genie runs on any device with a web browser. 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 by pressing the **On/Off** button.
2. Make sure that your device is connected with an Ethernet cable to your router.
3. Launch your Internet browser.
   - If this is the first time you are setting up the Internet connection for your router, the browser automatically goes to http://www.routerlogin.net, and the NETGEAR genie screen displays.
   - If you already used the NETGEAR genie, type **http://www.routerlogin.net** in the address field for your browser to display the NETGEAR genie screen. See *Use NETGEAR genie after Installation* on page 19.
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:

- Make sure that the computer is connected to one of the four LAN Ethernet ports, or wirelessly to the router.
- Make sure that the router is up and running. Its Wireless LEDs should turn on.
- Close and reopen the browser to make sure that the browser does not cache the previous page.
- Browse to **http://routerlogin.net**.
- If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the router.

If the router does not connect to the Internet:

1. Review your settings to be sure that you selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 9, 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 if you want to view or change settings for the router.

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

   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. See* *Types of Logins and Access on page 17* *for more information.*

Upgrade Router Firmware

When you set up your router and are connected to the Internet, the router automatically checks for you to see if newer firmware is available. If it is, a message is displayed on the top of the screen. See *Upgrade the Router Firmware* on page 66 for more information about upgrading firmware.

Click the message when it shows up, 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 and the Power LED has stopped blinking for several seconds.

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 six sections of the dashboard to view more detailed information. The left column has the menus, and at the top there is an Advanced tab that is used to access additional menus and screens.

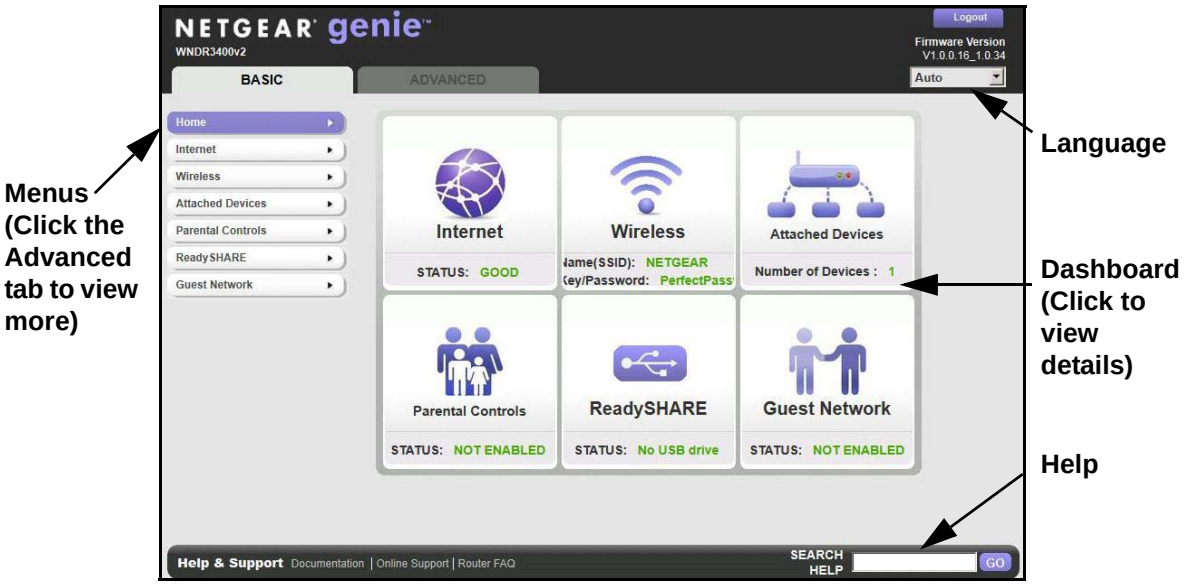


Figure 1. Router Basic Home screen with dashboard, language, and online help

- **Home**. This dashboard screen displays when you log in to the router.
- **Internet**. Set, update, and check the ISP settings of your router.
- **Wireless**. View or change the wireless settings for your router.
- **Attached Devices**. View the devices connected to your network.
- **Parental Controls**. Download and set up parental controls to prevent objectionable content from reaching your computers.
- **ReadySHARE**. If you connected a USB storage device to the router, then it is displayed here.
- **Guest Network**. Set up a guest network to allow visitors to use your router's Internet connection.
- **Advanced tab**. Set the router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 8, 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.

Add Wireless Devices or Computers to Your Network

Choose either the manual or the WPS method to add wireless devices and other equipment to your wireless network. See *Guest Networks* on page 31 for instructions on how to set up a guest network.

Manual Method

➢ **To connect manually:**

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

Wi-Fi Protected Setup (WPS) Method

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

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

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

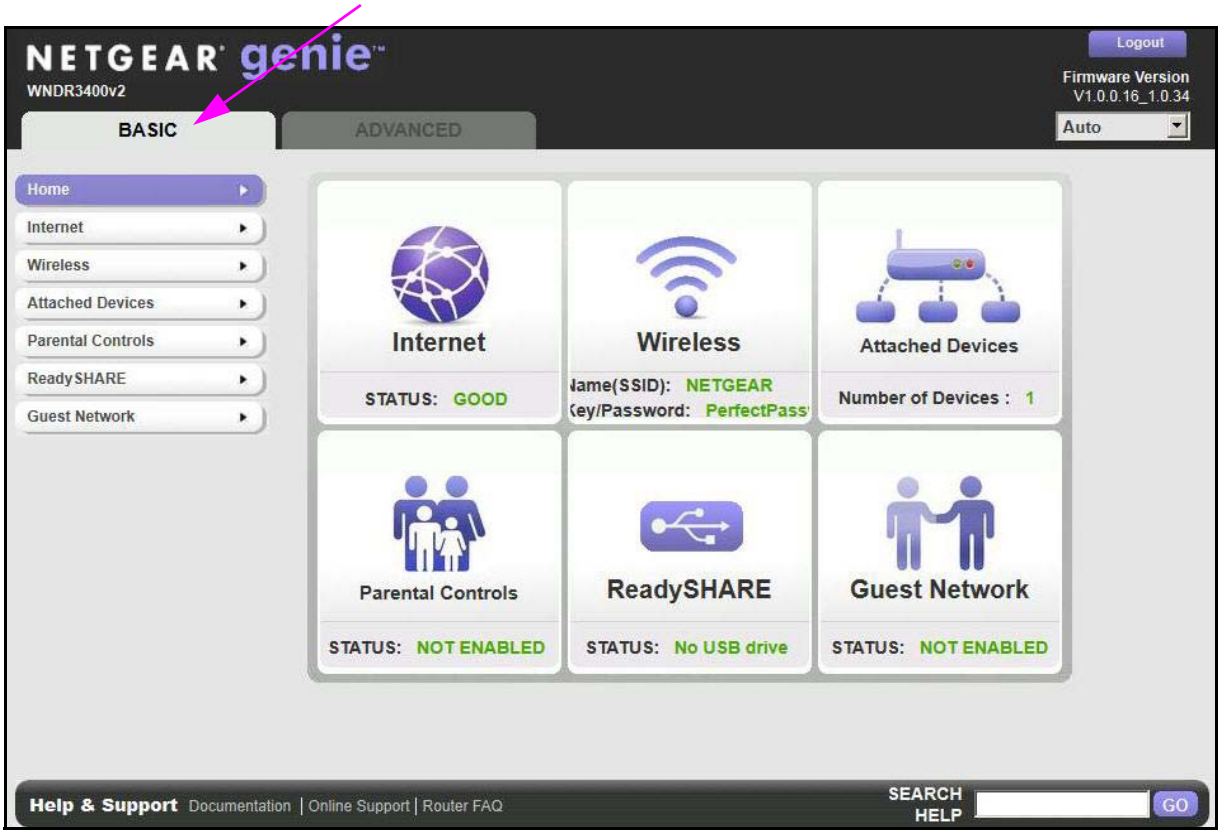
1. Press the **WPS** button on the router top panel .
2. Within 2 minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device. The device is now connected to your router.
3. Repeat steps 1–2 to add other WPS wireless devices.

genie Basic Settings

3

Your Internet connection and network

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



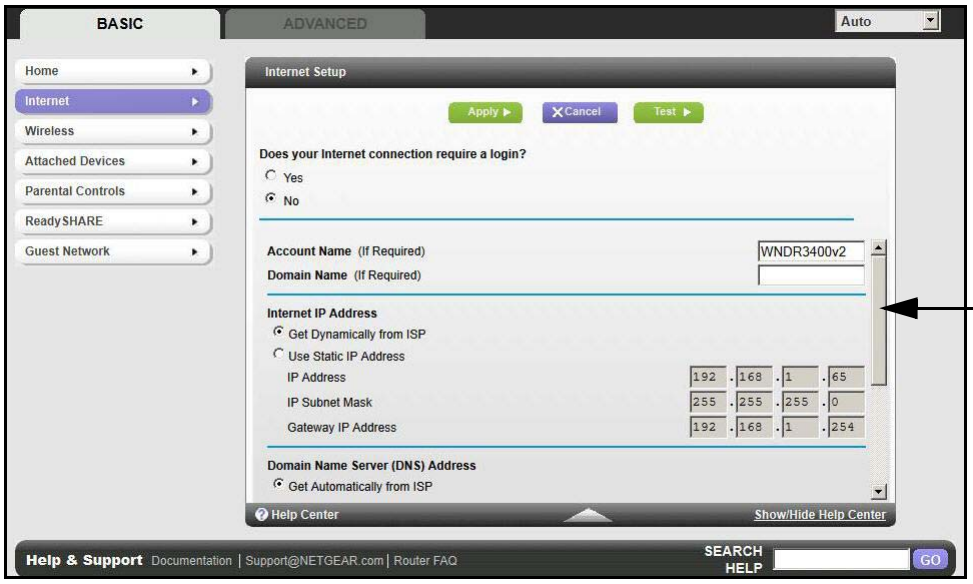
This chapter contains the following sections:

- *Internet Setup*
- *Attached Devices*
- *Parental Controls*
- *ReadySHARE USB Storage*
- *Basic Wireless Settings*
- *Guest Networks*

Internet Setup

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

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



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

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

2. Enter the settings for the IP address and DNS server. The default settings usually work fine. If you have problems with your connection, check the ISP settings.
3. Click **Apply** to save your settings.
4. Click **Test** to test your Internet connection. If the NETGEAR website does not display within 1 minute, see *Chapter 9, Troubleshooting*.

Internet Setup Screen Fields

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

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

These fields display when no login is required:

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

These fields display when your ISP requires a login:

- **Internet Service Provider Encapsulation**. ISP types. The choices are PPPoE, PPTP, or L2TP.
- **Login**. The login name provided by your ISP. This is often an email address.
- **Password**. The password that you use to log in to your ISP.
- **Idle Timeout (In minutes)**. If you want to change the login timeout, enter a new value in minutes. This 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.

- **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's router to which your router connects.

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

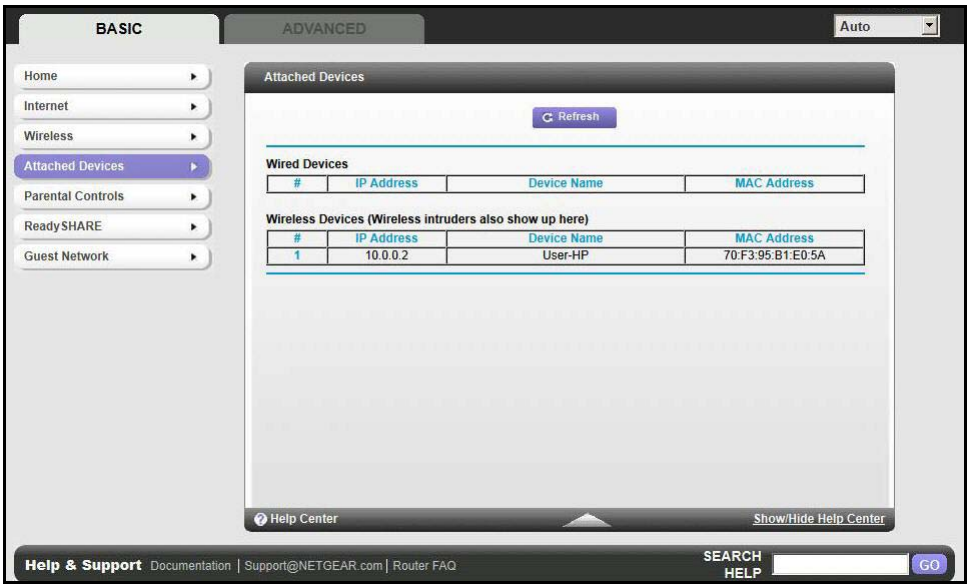
- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

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

- **Use Default Address**. Use the default MAC address.
- **Use Computer MAC Address**. The router captures and uses the MAC address of the computer that you are now using. You have to use the one computer that allowed by the ISP.
- **Use This MAC Address**. Enter the MAC address that you want to use.

Attached Devices

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



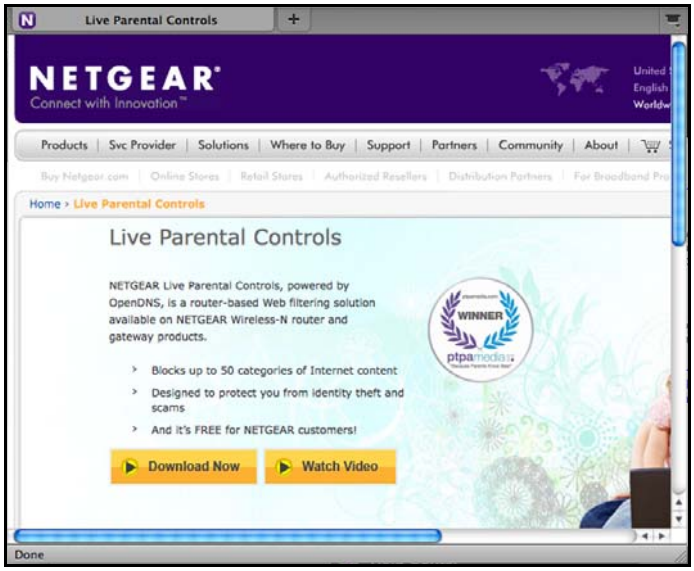
Wired devices are connected to the router with Ethernet cables. Wireless devices have joined the wireless network.

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

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

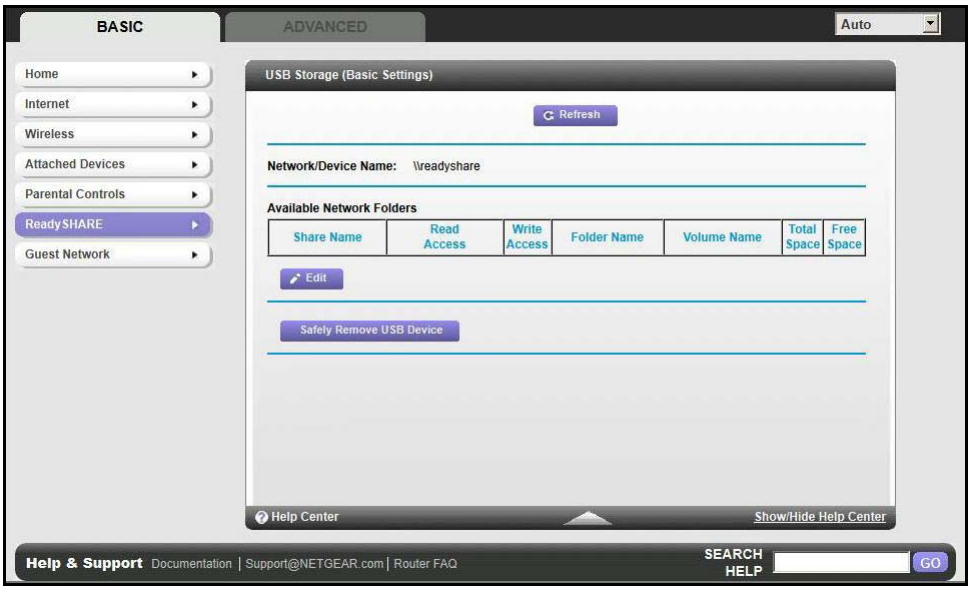
Parental Controls

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



ReadySHARE USB Storage

You can view information about a USB storage device that is connected to the router's USB port here. From the Basic Home screen, select **ReadySHARE** to display the USB Storage (Basic Settings) screen:



This screen displays the following:

- **Network/Device Name**. The default is \\readyshare. This is the name used to access the USB device connected to the router.
- **Available Network Folders**. The folders on the USB device.

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

  Read/Write Access. Shows the permissions and access controls on the network folder: All – no password (the default) allows all users to access the network folder. The user name (account name) for All – no password is guest. The password for admin is the same one that you use to log in to the router. By default, it is **password**.

  Folder Name. Full path used by the network folder.

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

  Total/Free Space. Shows the current utilization of the storage device.
- **Edit**. Click the **Edit** button to edit the Available Network Folders settings.
- **Safely Remove a USB Device**. Click to safely remove the USB device attached to your router.

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

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

Basic Wireless Settings

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

The N600 Wireless Dual Band Router comes with preset security. This means that the WiFi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the product label.

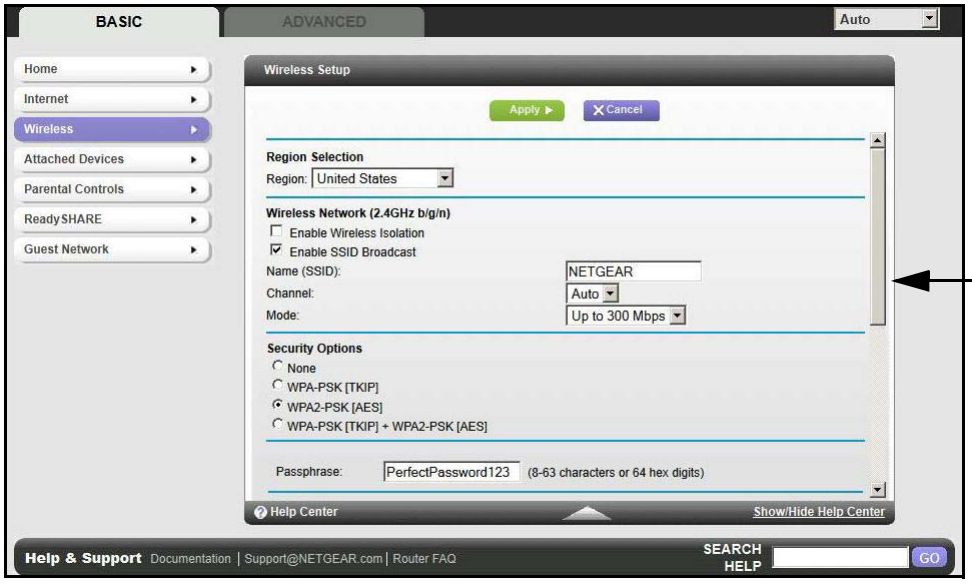
Note: The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

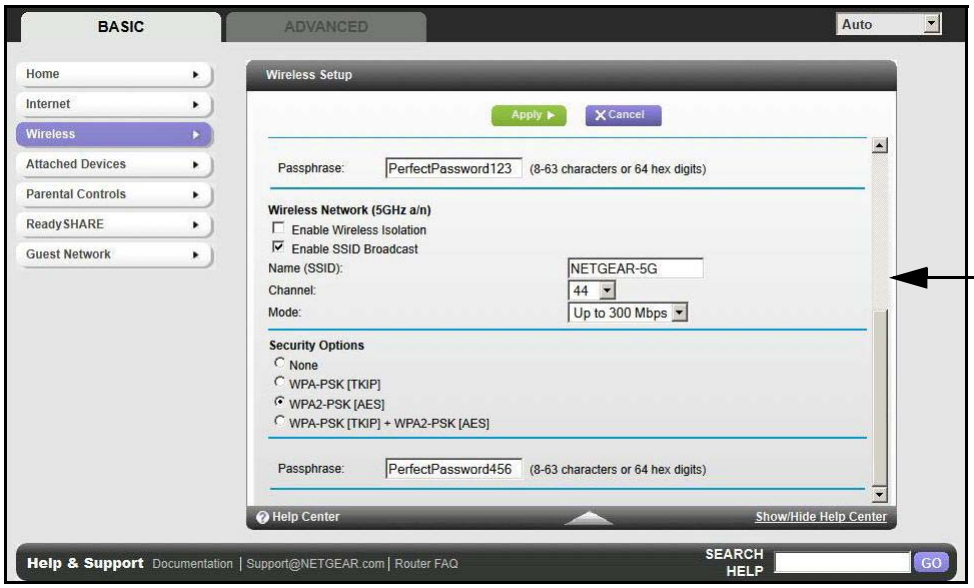
NETGEAR recommends that you do not change your preset security settings. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

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

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

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





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

2. Make any changes that are needed, and click **Apply** to save your settings.
3. Set up and test your wireless devices and computers to make sure that they can connect wirelessly. If they do not, check the following:
   - Is your wireless device or computer connected to your network or another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.

- Does your wireless device or computer 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 Setup Screen Fields

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

Wireless Network

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

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 **Allow Broadcast of Name (SSID)** check box, and click **Apply**.

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

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.***

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

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

Security Options Settings

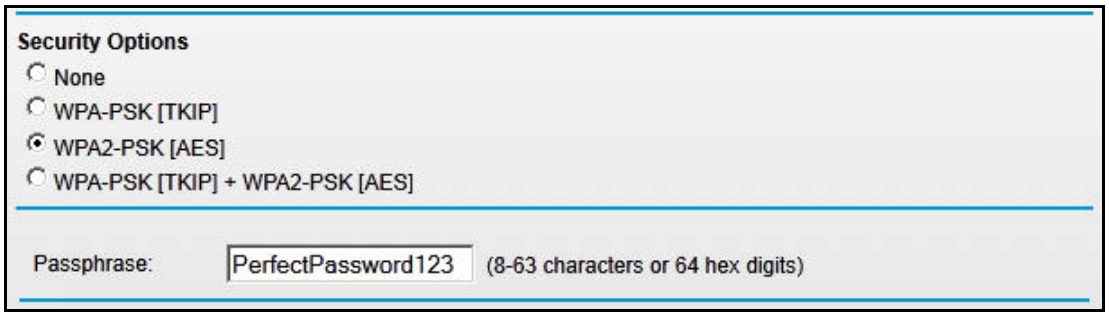
> **Note:** These settings apply separately to the 2.4 GHz b/g/n and 5 GHz a/n bands.

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

Change WPA Security Option and Passphrase

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

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



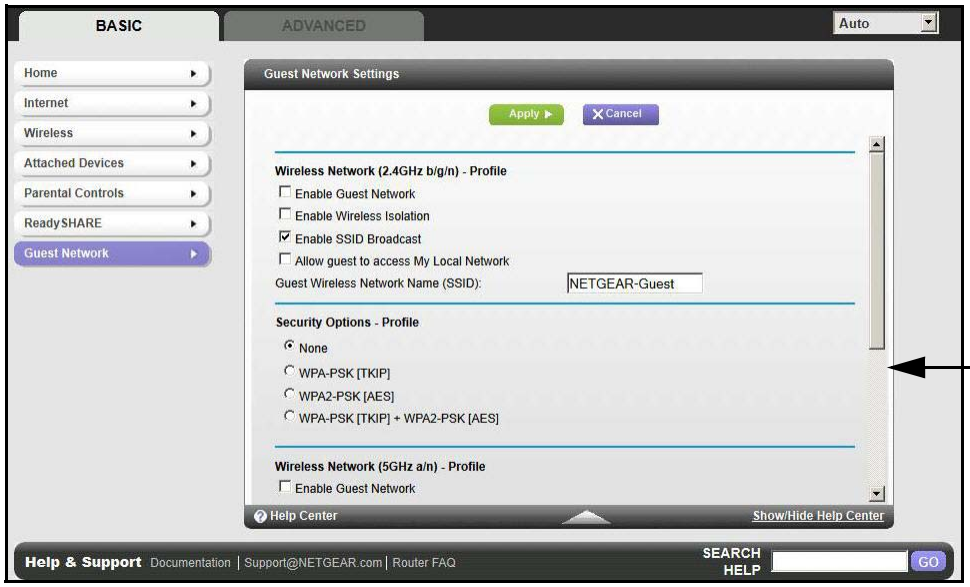
2. In the Passphrase field that displays when you select a WPA security option, enter the network key (passphrase) that you want to use. It is a text string from 8 to 63 characters.

Guest Networks

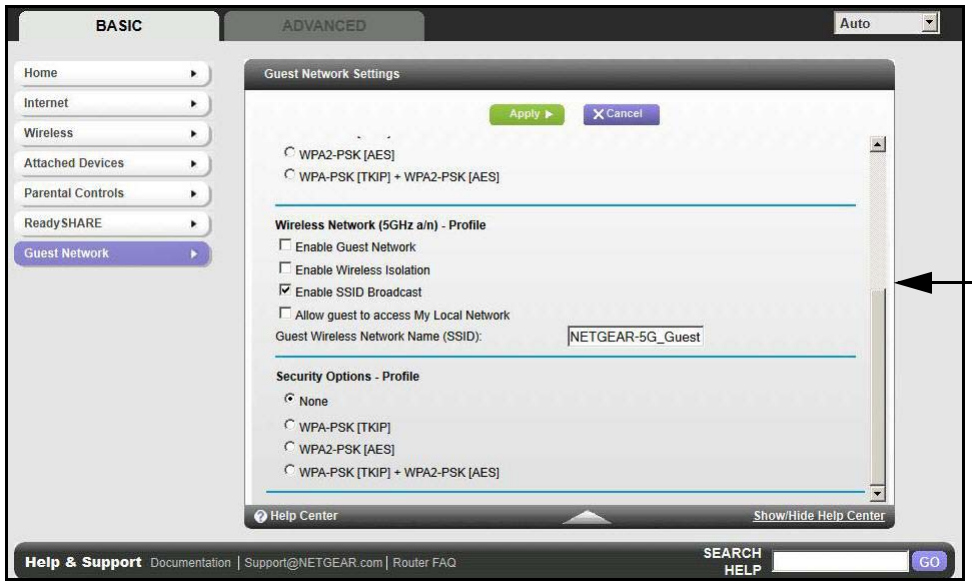
Adding a guest network allows visitors at your home to use the Internet without providing them with your wireless security key. You can add a guest network to each wireless network: 2.4 GHz b/g/n and 5.0 GHz a/n.

➢ **To set up a guest network:**

1. Select **Basic > Guest Network** to display the following screen:



Scroll to view more settings



Scroll to view more settings

2. Select any of the following wireless settings:

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

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

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

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

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

3. Give the guest network a name.

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

4. Select a security option from the list. The security options are described in *Guest Network Wireless Security Options* on page 32.
5. Click **Apply** to save your selections.

Guest Network Wireless Security Options

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

This section presents an overview of the security options and provides guidance on when to use which option. Note that it is also possible to set up a guest network without wireless security. NETGEAR does *not* recommend this.

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

WPA-PSK uses a passphrase to 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 is designed to work with all wireless network interface cards, but not all wireless access points. It is superseded by WPA2-PSK.

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

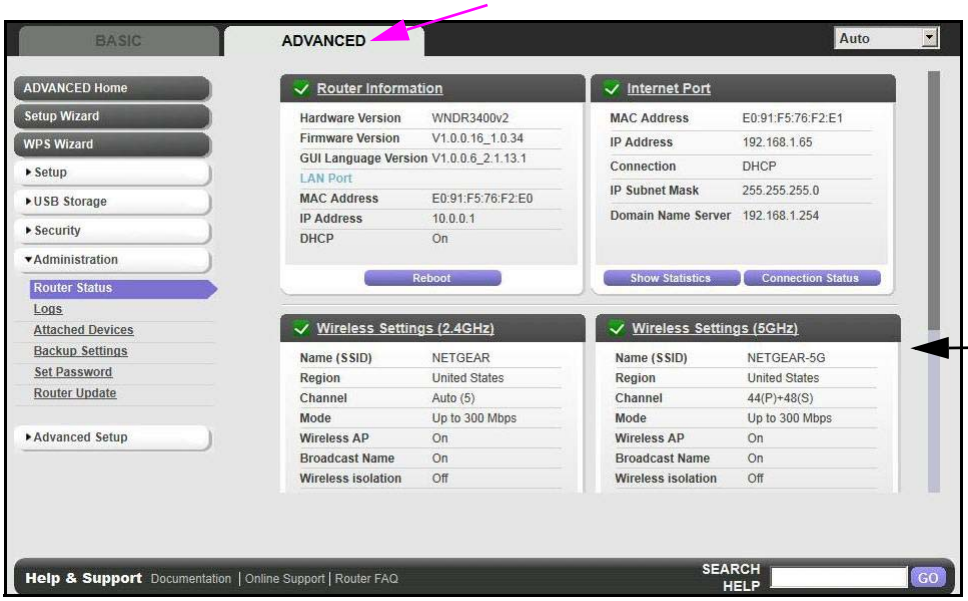
WPS-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. The product documentation for your wireless adapter and WPA client software should have instructions about configuring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

genie Advanced Home

4

Specifying custom settings

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



This screen is also displayed through the Administration menu.

This chapter contains the following sections:

- *Setup Wizard*
- *WPS Wizard*
- *Setup Menu*
- *WAN Setup*
- *LAN Setup*
- *Quality of Service (QoS) Setup*

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

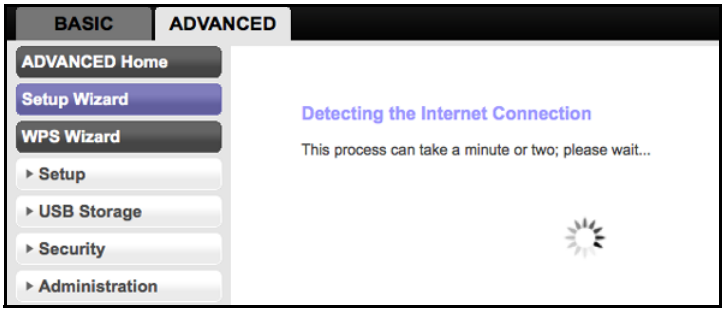
- **USB Storage**. See *Chapter 5, USB Storage*.
- **Security**. See *Chapter 6, Security*.
- **Administration**. See *Chapter 7, Administration*.
- **Advanced Setup**. See *Chapter 8, Advanced Settings*.

Setup Wizard

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

1. Select **Setup Wizard** to display the following screen:

2. Select either **Yes** or **No, I want to configure the router myself**. If you select No, you are taken to the Internet Setup screen (see *Internet Setup* on page 23).
3. If you selected Yes, click **Next**. The following screen displays:



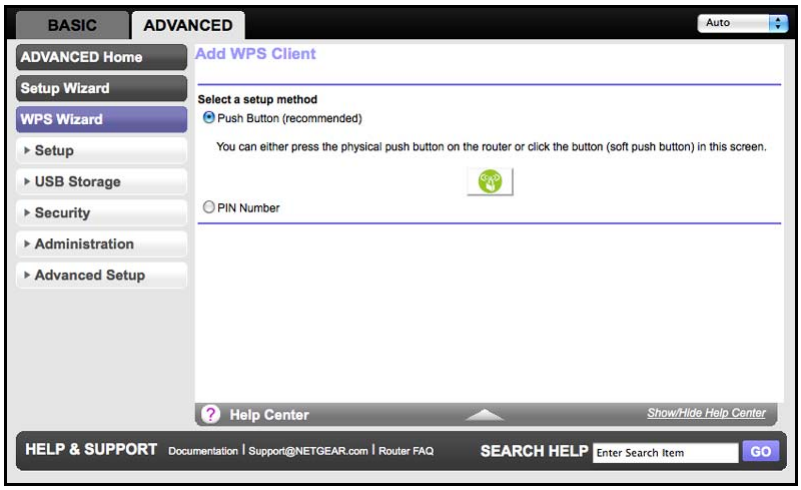
The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. The following screen displays:

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, you need to either press its WPS button or locate its WPS PIN.

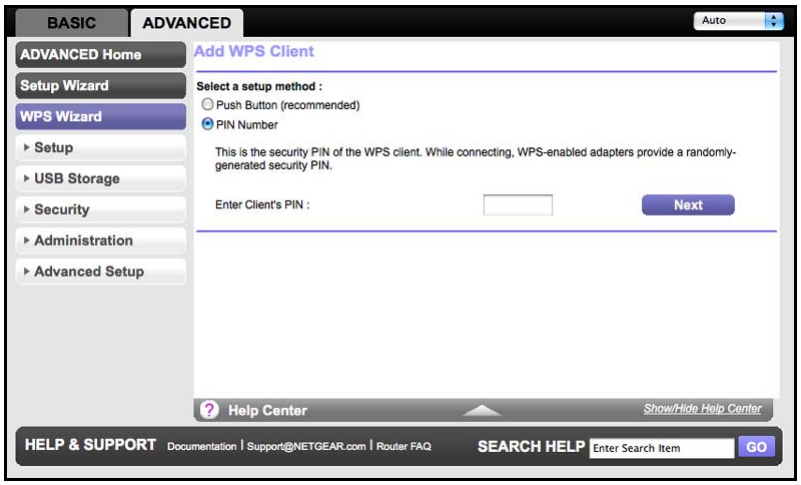
To use the WPS Wizard:

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



You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.
   - To use the push-button method, either click the **WPS** button on this screen, or press the **WPS** button on the top of the router. Within two minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.
   - To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click **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 LED on the top of the router blinks green. When the router establishes a WPS connection, the LED is solid green, and the router WPS screen displays a confirmation message.

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

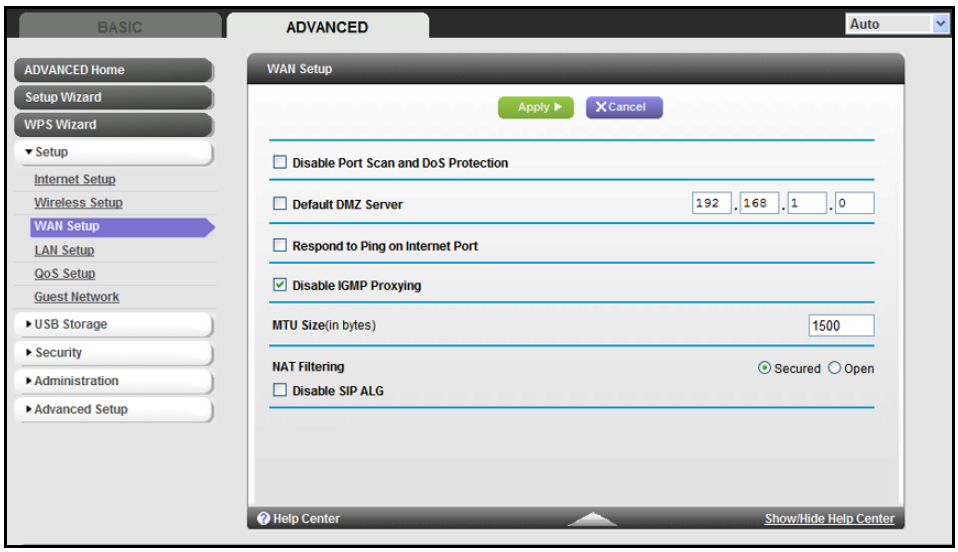
Setup Menu

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

- **Internet Setup**. This is a shortcut to the same Internet Setup screen that you can access from the dashboard on the Basic Home screen. See *Internet Setup* on page 23.
- **Wireless Setup**. This is a shortcut to the same Wireless Setup screen that you can access from the dashboard on the Basic Home screen. See *Basic Wireless Settings* on page 27.
- **Guest Network**. This is a shortcut to the same Guest Network screen that you can access from the dashboard on the Basic Home screen. See *Guest Networks* on page 31.
- **WAN Setup**. Internet (WAN) setup. See *WAN Setup* on page 38.
- **LAN Setup**. Local area network (LAN) setup. See *LAN Setup* on page 41.
- **QoS Setup**. Quality of Service (QoS) setup. See *Quality of Service (QoS) Setup* on page 44.

WAN Setup

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



- **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This should be disabled only in special circumstances.
- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, *Default DMZ Server*, for more details.
- **Respond to Ping on Internet Port**. If you want the router to respond to a ping from the Internet, select this check box. Use this only as a diagnostic tool because it allows your router to be discovered. Do not select this check box unless you have a specific reason.
- **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. This 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 39.
- **NAT Filtering**. Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function.

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

WARNING!

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

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

➢ **To set up a default DMZ server:**

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

Change the MTU Size

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

The best MTU setting for NETGEAR equipment is often just the default value, and changing the value might fix one problem but cause another. Leave the MTU unchanged unless one of these situations occurs:

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

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

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

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

Table 2. Common MTU sizes

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

➢ **To change the MTU size:**

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

LAN Setup

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

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

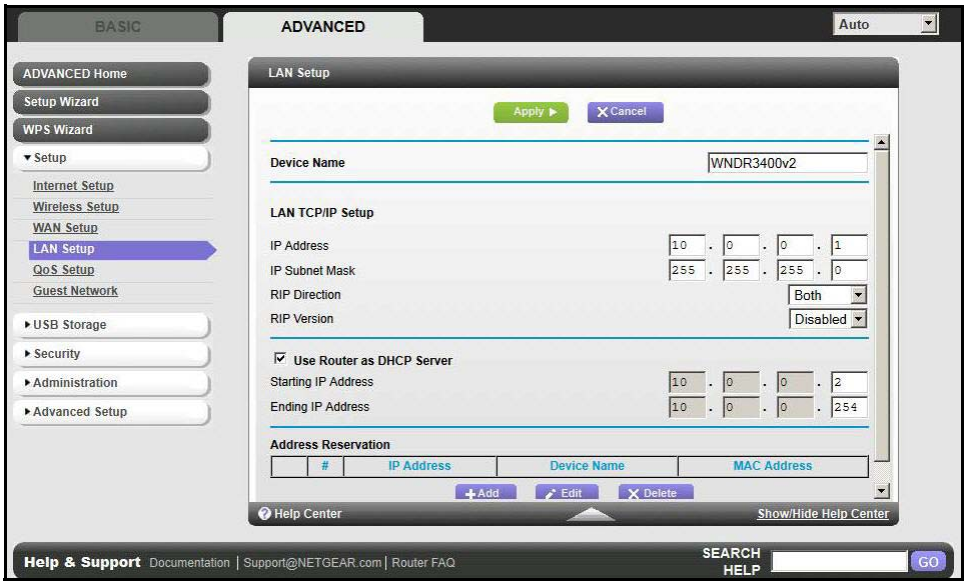
- LAN IP address: **192.168.1.1**
- Subnet mask: **255.255.255.0**

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

➢ **To change the LAN settings:**

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

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



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

LAN Setup Screen Settings

LAN TCP/IP Setup

- **IP Address**. The LAN IP address of the router.
- **IP Subnet Mask**. The LAN subnet mask of the router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or router.
- **RIP Direction**. Router Information Protocol (RIP) allows a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. Both is the default setting. With the Both or Out Only setting, the router broadcasts its routing table periodically. With the Both or In Only setting, the router incorporates the RIP information that it receives.
- **RIP Version**. This 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 usually selected so that the router functions as a Dynamic Host Configuration Protocol (DHCP) server.

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

Address Reservation

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

Use the Router as a DHCP Server

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

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

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

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

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

Address Reservation

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

➢ **To reserve an IP address:**

1. In the Address Reservation section of the screen, click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the router's LAN subnet, such as 192.168.1.x.)
3. Type the MAC address of the computer or server.

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

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

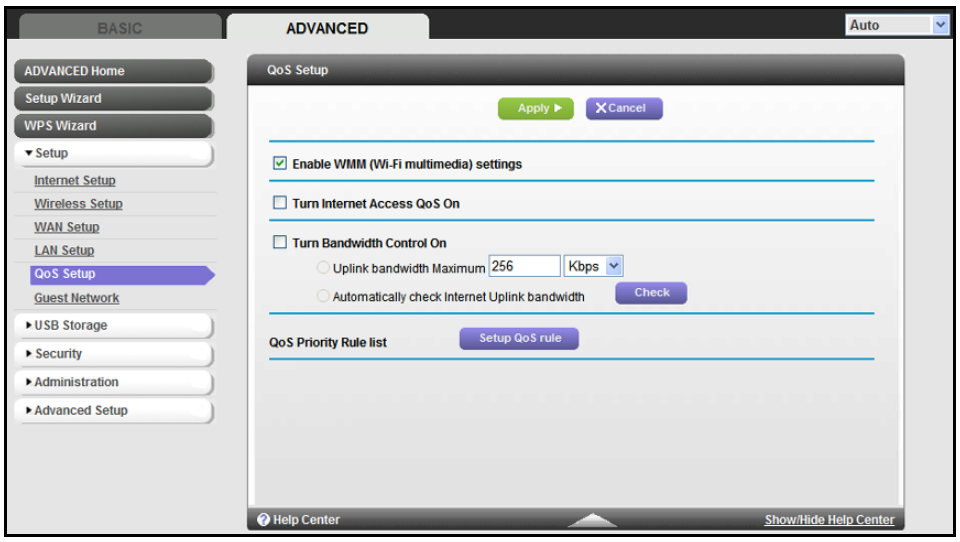
   The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

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

Quality of Service (QoS) Setup

QoS is an advanced feature that can be used to prioritize some types of traffic ahead of others. The N600 Wireless Dual Band Router can provide QoS prioritization over the wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen.

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



Enable WMM QoS for Wireless Multimedia Applications

The N600 Wireless Dual Band Router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both the application and the client running that application must have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS are assigned to the best effort category, which receives a lower priority than voice and video.

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

Set Up QoS for Internet Access

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

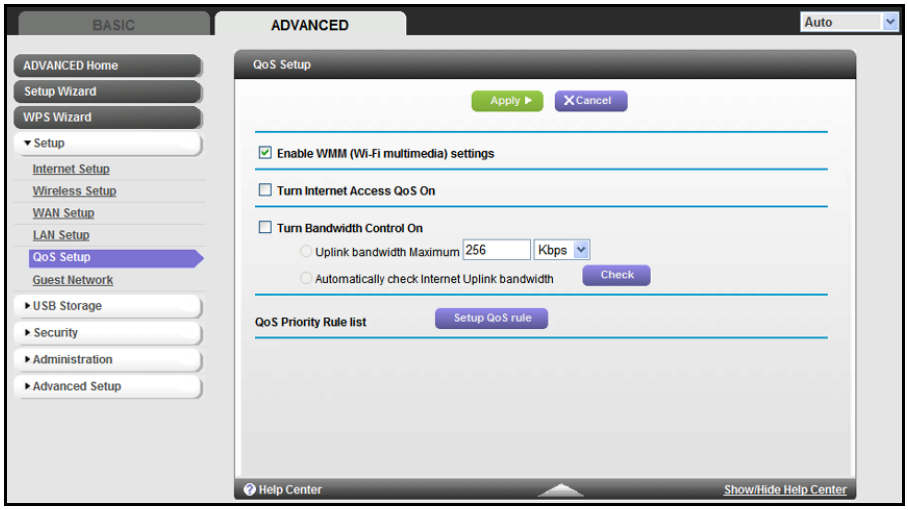
- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the router
- A specific device by MAC address

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

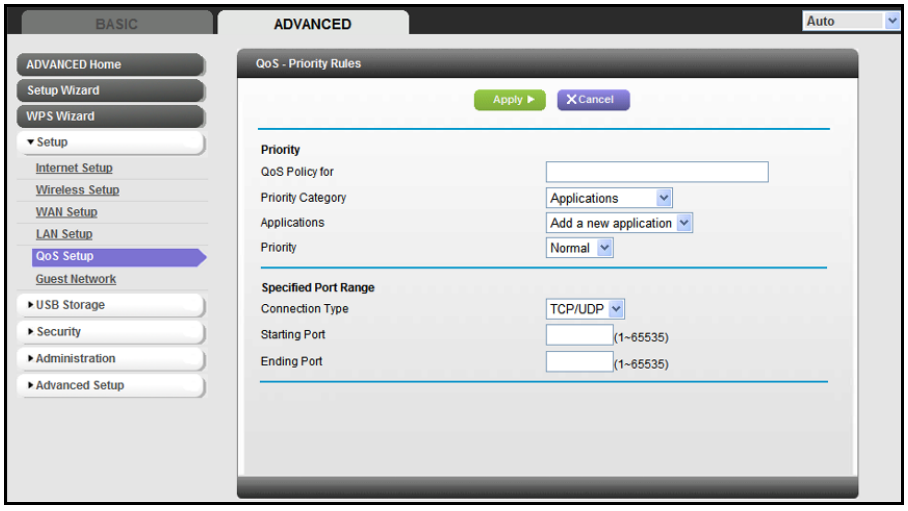
QoS for Applications and Online Gaming

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

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

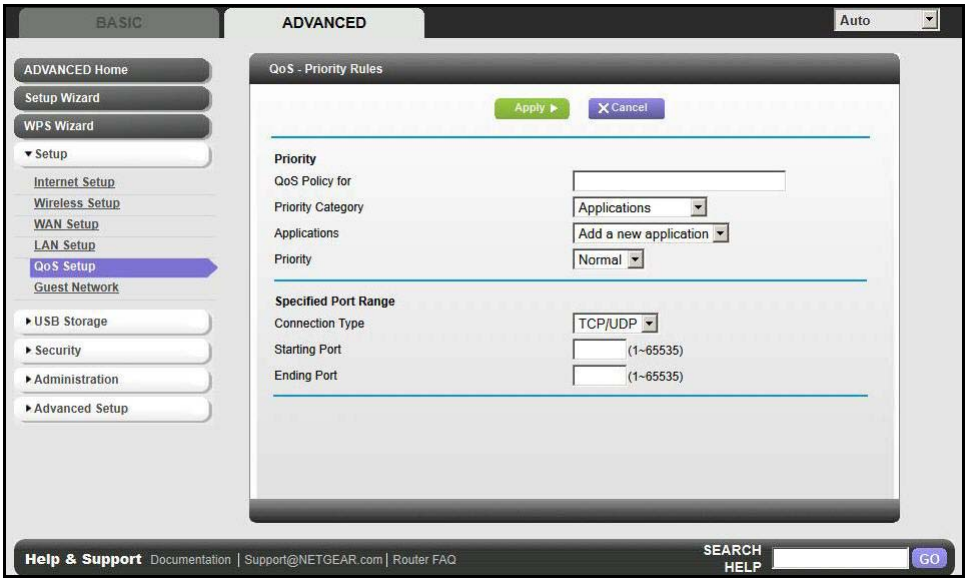


3. To add a priority rule, scroll down to the bottom of the QoS Setup screen and click **Add Priority Rule** to display the following screen:



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

5. In the Priority Category list, select either **Applications** or **Online Gaming**. In either case, a list of applications or games displays in the list.
6. You can select an existing item from the list, or you can scroll and select **Add a New Application** or **Add a New Game**, as applicable.
   a. If you add a new entry, the Priority Rules screen expands as shown:



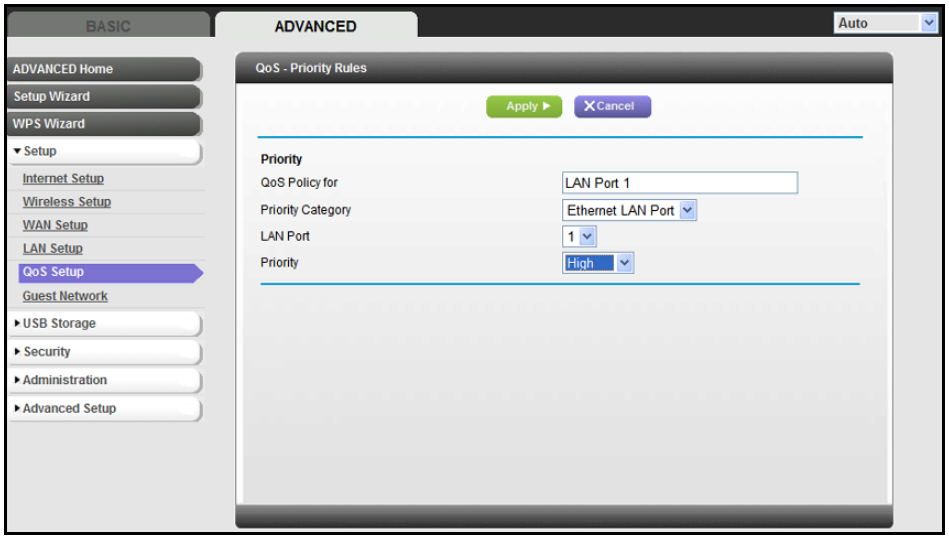
   b. In the QoS Policy for field, enter a descriptive name for the new application or game.
   c. In the Connection Type list, select either **TCP, UDP,** or both (**TCP/UDP**), and specify the port number or range of port numbers used by the application or game.
7. From the Priority list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
8. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

QoS for a 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** to display the QoS Setup screen. Select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button.
3. Click the **Add Priority Rule** button.

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

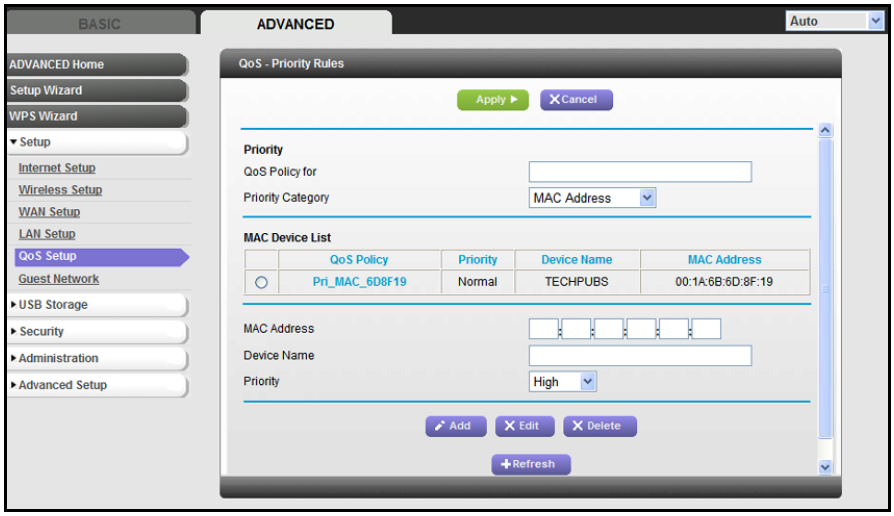


5. From the LAN port list, select the LAN port that will have a QoS policy.
6. From the Priority list, select the priority that this port's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
7. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
8. In the QoS Setup screen, click **Apply**.

QoS for a MAC Address

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

1. Select **Advanced > Setup > QoS Setup**, and click the **Setup QoS Rule** button. The QoS Setup screen displays.
2. Click **Add Priority Rule**.
3. From the Priority Category list, select **MAC Address** to display the following screen:



4. If the device to be prioritized appears in the MAC Device List, select its radio button. The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, you have to complete these fields manually.
5. From the Priority list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest. Click **Add** to add this rule to MAC Device List.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
8. Click **Apply**.

Editing or Deleting an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

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

USB Storage

5

Accessing and configuring a USB storage drive

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

This chapter contains the following sections:

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

USB Drive Requirements

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

Table 3. USB Drive Speeds

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

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

http://kbserver.netgear.com/readyshare

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

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

ReadySHARE Access

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

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

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

File-Sharing Scenarios

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

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

A few common uses are described in the following sections.

Sharing Photos

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

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

1. Insert your USB drive into the USB port on the router either directly or with a USB cable.

   Computers on your local area network (LAN) can automatically access this USB drive using a web browser or Microsoft Networking.

2. If you want to specify read-only access or to allow access from the Internet, see *USB Storage Advanced Settings* on page 54.

Storing Files in a Central Location for Printing

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

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

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

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

Sharing Large Files over the Internet

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

Sharing files with a remote colleague involves the following considerations:

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

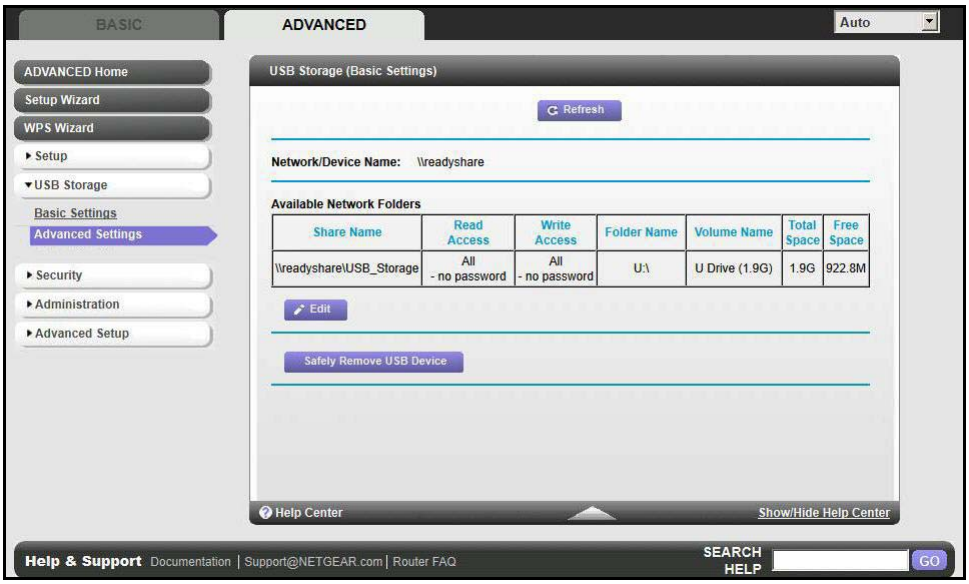
Note: You can enable the HTTP (via Internet) option on the USB Storage (Advanced Settings) screen to share large files. This option supports downloading files only.

Basic Settings

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

You can access this feature through **Basic > ReadySHARE**, or through **Advanced > USB Storage > ReadySHARE**.

The USB Storage (Basic Settings) screen displays:



By default, the USB storage device is available to all computers on your local area network (LAN).

➢ **To access your USB device:**

1. Click the network device name or the share name in your computer's network folders list.
2. For SMB://readyshare, click **Connect**.

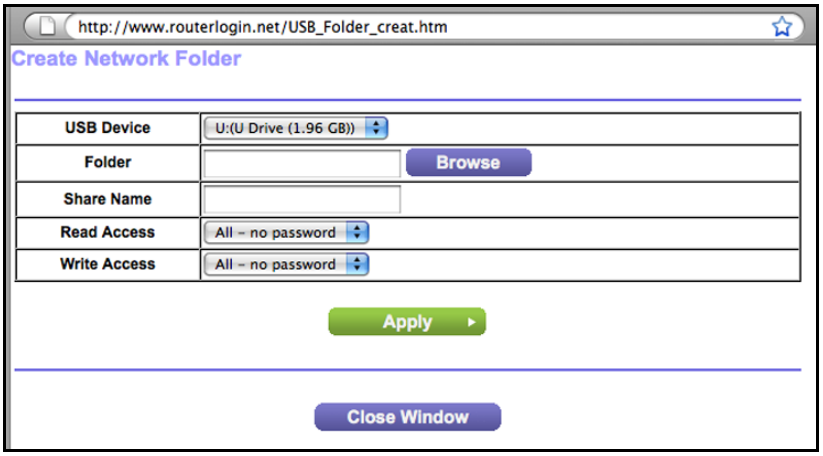
Note: If you logged in to the router before you connected your USB device, you might not see your USB device in the router screens until you log out and then log back in again.

Add or Edit a Network Folder

1. You can access this feature by selecting **Basic > ReadyShare > Edit**, or **Advanced > USB Storage > Advanced Settings**.

2. Specify the changes that you want to make:

- To add a folder, click **Create Network Folder**.



- To edit a folder, select its radio button, and click **Edit**.

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

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

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

USB Storage Advanced Settings

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

You can use this screen to specify access to the USB storage device.

- **Network Device Name**. The default is readyshare. This is the name used to access the USB device connected to the router.
- **Workgroup**. If you are using a Windows workgroup rather than a domain, the workgroup name is displayed here. The name works only in an operating system that supports NetBIOS, such as Microsoft Windows.
- **Access Method**. The access methods are described here.

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

  HTTP. Enabled by default. You can type **http://readyshare.routerlogin.net/shares** to access the USB drive.

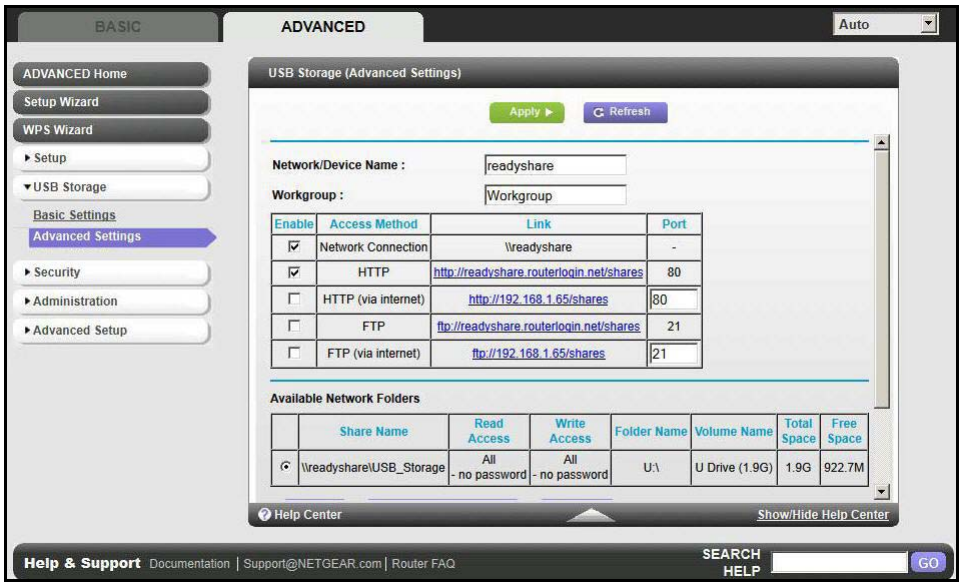
  HTTP (via Internet). Disabled by default. If you enable this setting, remote users can type **http://*<public IP address>*/shares** (for example, **http://1.1.10.102/shares**) or a URL domain name to access the USB drive over the Internet. This setting supports file uploading only.

  FTP. Disabled by default.

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

Available Network Folders

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



- **Share Name**. If only 1 device is connected, the default share name is USB_Storage. You can click the name shown, or you can type it in the address field of your web browser. If Not Shared is shown, the default share has been deleted, and no other share for the root folder exists. Click the link to change this setting.

- **Read/Write Access**. Shows the permissions and access controls on the network folder: All - no password (the default) allows all users to access the network folder. The password for admin is the same one that you use to log in to the router.
- **Folder Name**. Full path used by the network folder.
- **Volume Name**. Volume name from the storage device (either USB drive or HDD).
- **Total/Free Space**. Shows the current utilization of the storage device.

Safely Remove a USB Drive

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

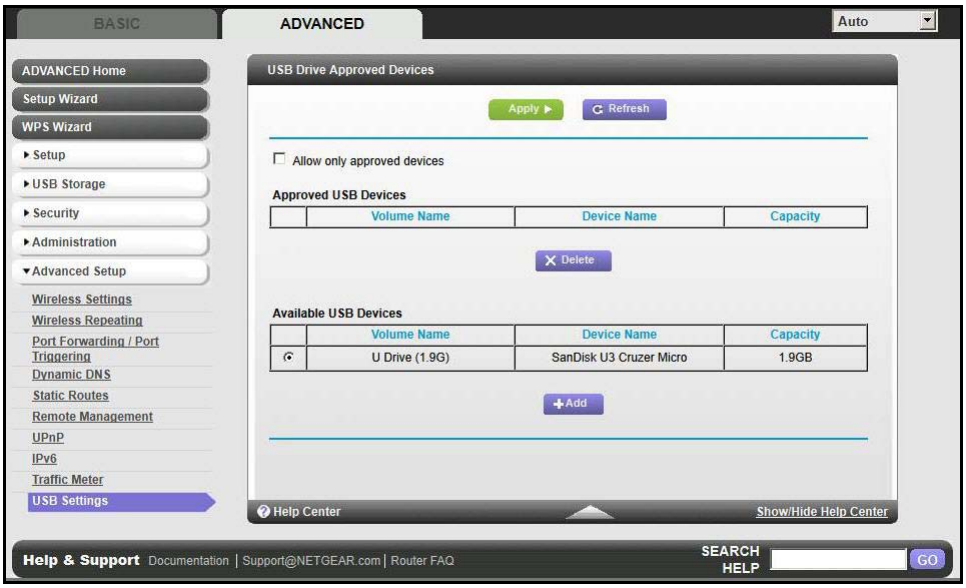
Specify Approved USB Devices

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

➢ **To set up approved USB devices:**

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

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



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

3. To add an approved USB device, select it from the Available USB Devices list and click **Add**.
4. Select the **Allow only approved devices** check box.
5. Click **Apply** so that your change takes effect.

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

Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers with a web browser, you have to use the router's Internet port IP address. If you are using Dynamic DNS, you can type the DNS name rather than the IP address. You can view the router's Internet IP address from the dashboard on the Basic Home screen or the Advanced Home screen.

Access the Router's USB Drive Remotely Using FTP

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

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

   ftp://10.1.65.4

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

2. Type the account name and password that has access rights to the USB drive. The user name (account name) for All – no password is **guest**.
3. The directories of the USB drive that your account has access to are displayed, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Security

6

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 PCs and other devices connected to your network.

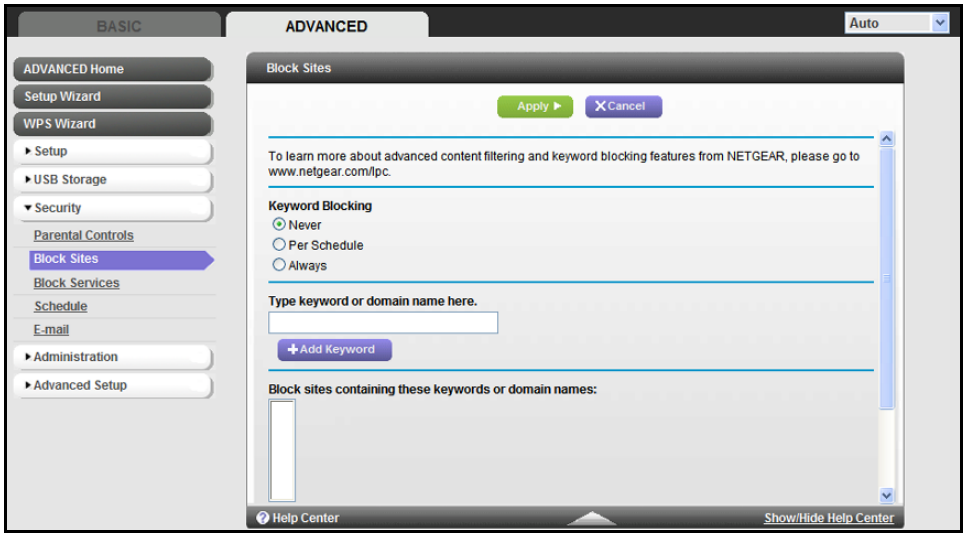
This chapter includes the following sections:

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

Keyword Blocking of HTTP Traffic

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

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



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

   The Keyword list supports up to 32 entries. Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (.) to block all Internet browsing access.

➢ **To delete a keyword or domain:**

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

➢ **To specify a trusted computer:**

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

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

Block Services (Port Filtering)

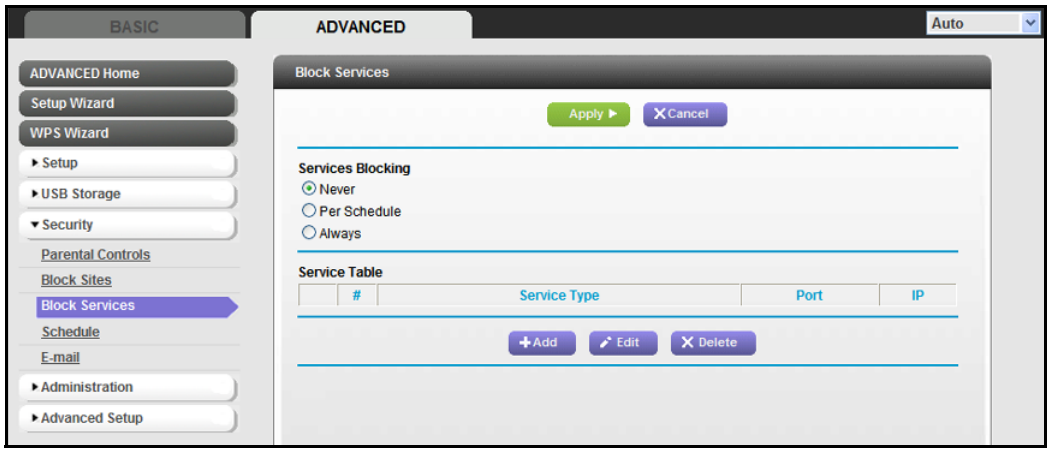
Services are functions performed by server computers at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server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

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. Although the router already holds a list of many service port numbers, you are not limited to these choices. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

The Block Services screen lets you add and block specific Internet services by computers on your network. This is called service blocking or port filtering. To add a service for blocking, first determine which port number or range of numbers use the application.

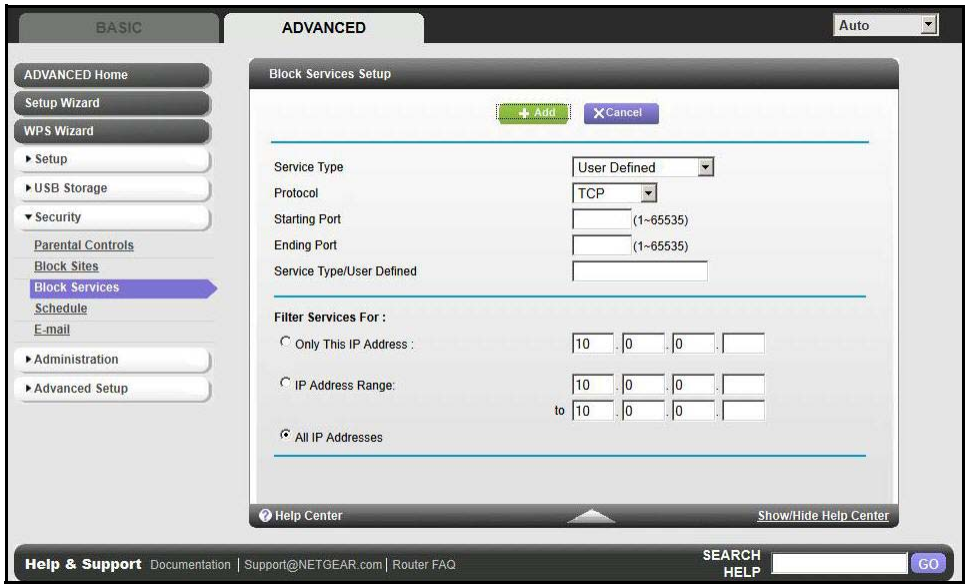
➢ **To block services:**

1. Select **Advanced > Security > Block Services** to display the following screen:



2. Select either **Per Schedule** or **Always** to enable service blocking, and click **Apply**. If you selected Per Schedule, specify a time period in the Schedule screen as described in *Schedule Blocking* on page 62.

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



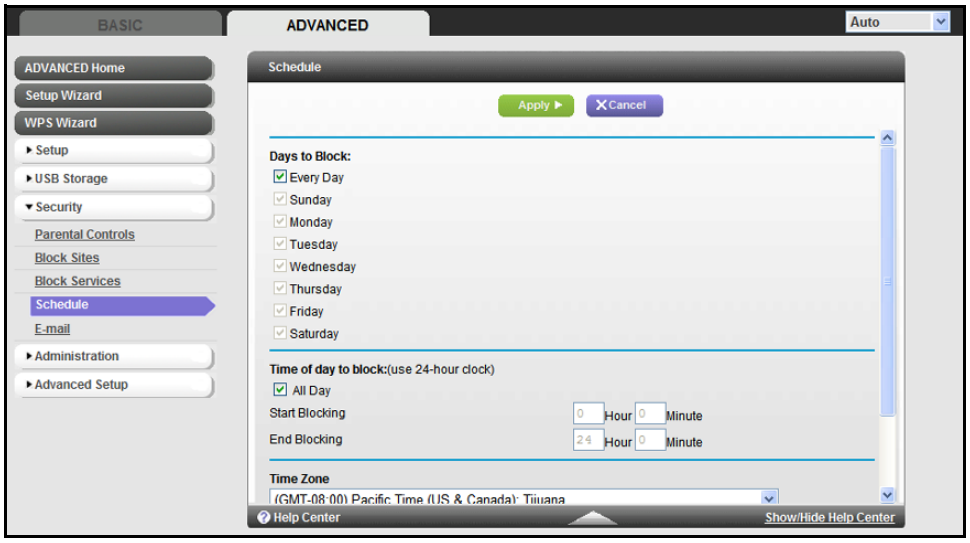
4. From the Service Type list, select the application or service to allow or block. The list already displays several common services, but you are not limited to these choices. To add additional services or applications that do not already appear, select **User Defined.**
5. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.
6. Enter the starting and ending port numbers. If the application uses a single port number, enter that number in both fields.
7. Select the radio button for the IP address configuration you want to block and enter the IP addresses. You can block the specified service for a single computer, a range of computers with consecutive IP addresses, or all computers on your network.
8. Click **Add** to enable your Block Services Setup selections.

Schedule Blocking

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

➢ **To schedule blocking:**

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



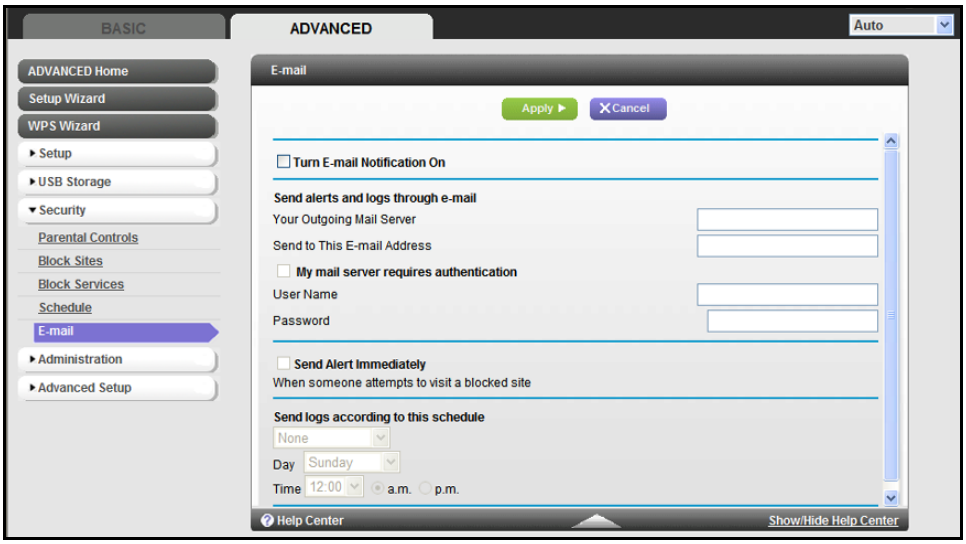
2. Set up the schedule for blocking keywords and services.
   - **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** to select the check boxes for all days.
   - **Time of Day to Block**. Select a start and end time in 24-hour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

Security Event Email Notifications

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

➢ **To set up email notifications:**

1. Select **Advanced > Security > Email** to display the following screen:



2. To receive email logs and alerts from the router, select the **Turn Email 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. Enter the email address to which logs and alerts are sent in the Send to This Email Address field. This email address is also used for the From address. If you leave this field blank, log and alert messages are not sent by email.
5. If your outgoing email server requires authentication, select the **My Mail Server requires authentication** check box. Fill in the User Name and Password fields for the outgoing email server.
6. You can have email alerts sent immediately when someone attempts to visit a blocked site and you can specify that logs are sent automatically.

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

Administration

7

Managing your network

This chapter describes the router settings for administering and maintaining your router and home network. See *Remote Management* on page 95 for information about upgrading or checking the status of your router over the Internet. See *Traffic Meter* on page 98 for information about monitoring the volume of Internet traffic passing through your router's Internet port.

This chapter includes the following sections:

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

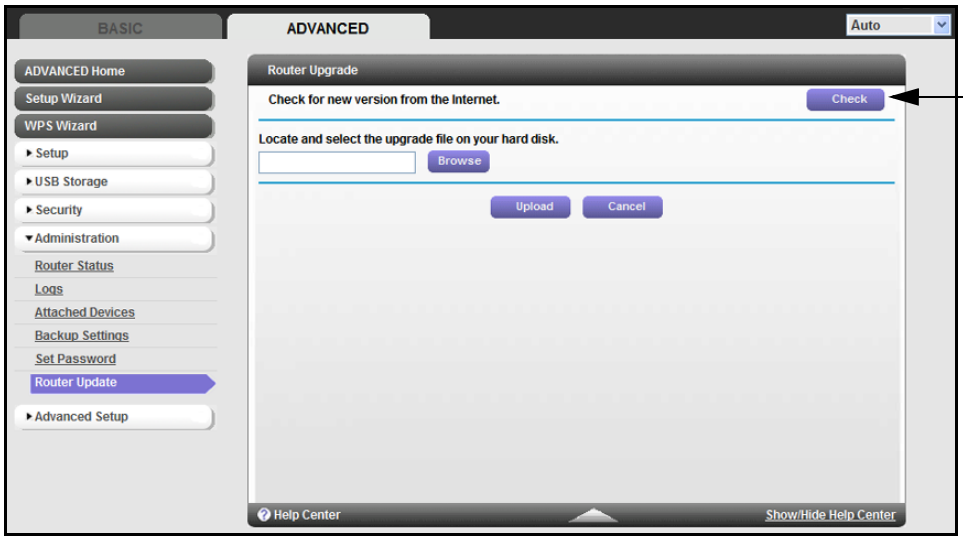
Upgrade the Router Firmware

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 Router Update screen to check and update to the latest firmware for your product.

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

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



2. Click **Check**.

   The router finds new firmware if available.

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

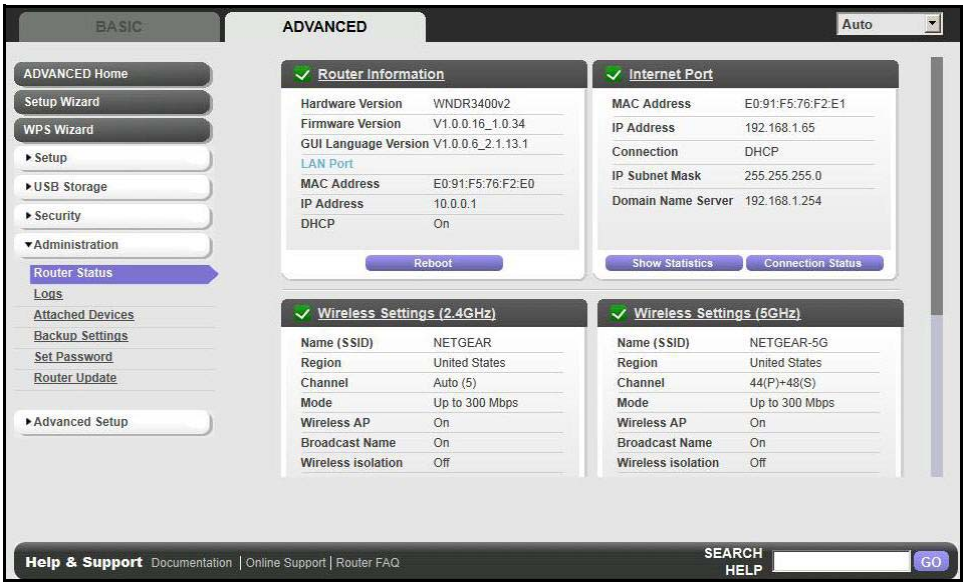
WARNING!

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

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

View Router Status

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



Router Information

Hardware Version. The router model.

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

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

LAN Port.

- **MAC Address**. The Media Access Control address is the unique physical address used by the Ethernet (LAN) port of the router.
- **IP Address**. The IP address used by the Ethernet (LAN) port of the router. The default is 192.168.1.1.
- **DHCP Server**. Identifies whether the router's built-in DHCP server is active for the LAN-attached devices.

Internet Provider (WAN) Setup

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

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

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

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

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

Statistics Button

On the Router Status screen, in the Internet Provider (WAN) Setup pane, click the **Statistics** button to display the following screen:

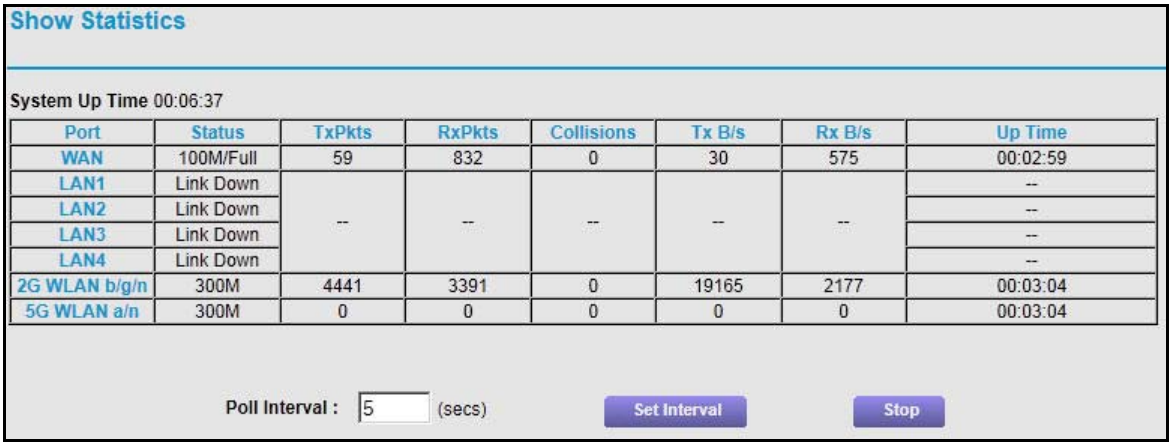


Figure 2. System up time and poll interval statistics

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

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

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

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

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

Connection Status Button

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

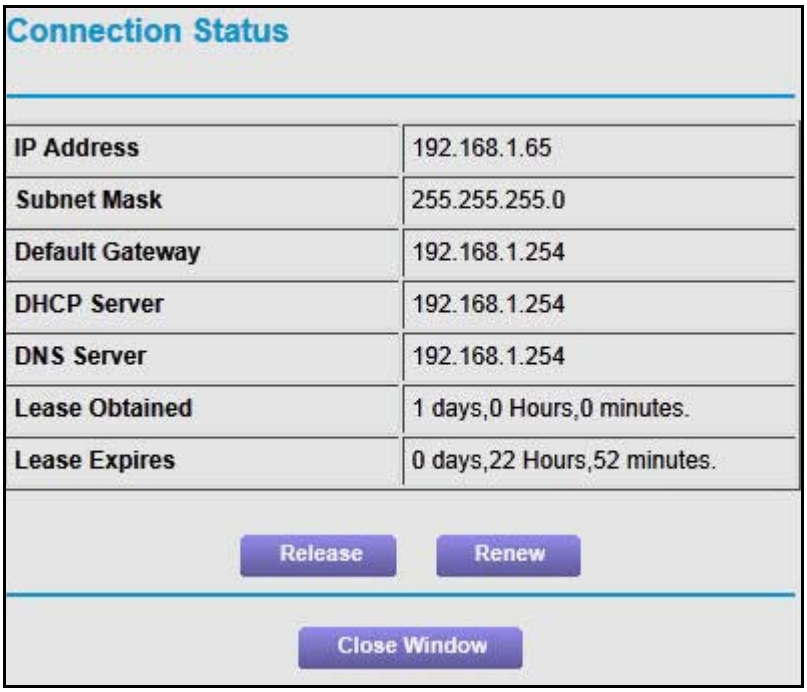


Figure 3. View connection status information

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

IP Address. The IP address assigned to the router.

Subnet Mask. The subnet mask assigned to the router.

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

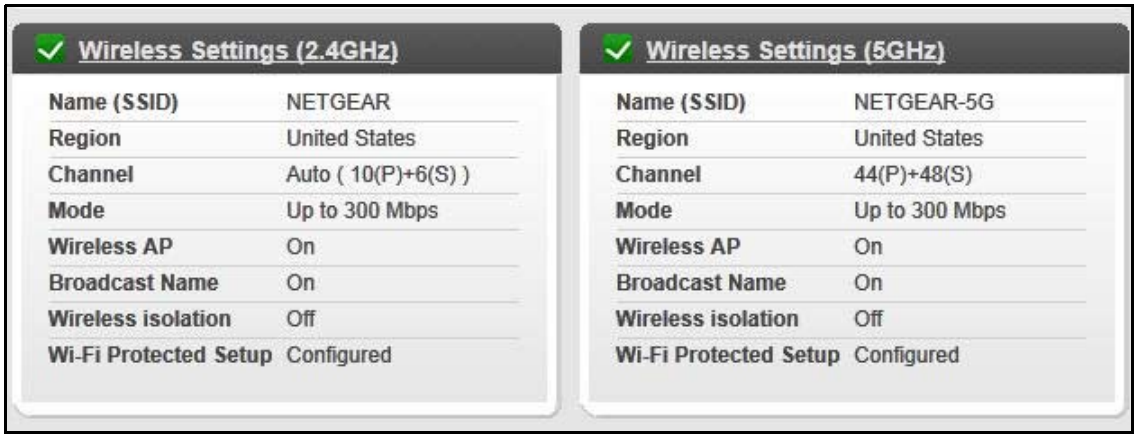
DHCP Server. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.

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.

Wireless Settings (2.4 GHz and 5 GHz)



The following settings are displayed:

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

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

Channel. Identifies the operating channel of the wireless port being used. The default channel is Auto. When Auto is selected, the 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 donot interfere with each other.

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

Wireless AP. Indicates whether the radio feature of the 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. Select this check box only if you want to prevent wireless connections to the router.

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

Guest Network (2.4 GHz and 5 GHz)

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

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

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

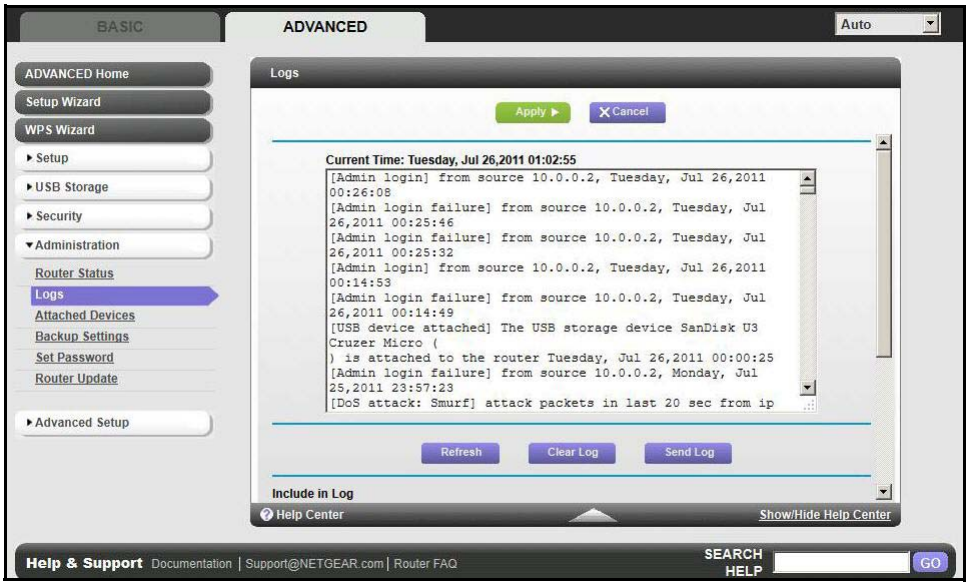
Wireless Isolation. Select this check box only if you want to prevent wireless connections to the router.

Allow guest to access My Local Network. If selected, any user who connects to this SSID can access local networks associated with the router.

View Logs of Web Access or Attempted Web Access

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

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



The log 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.

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

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

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

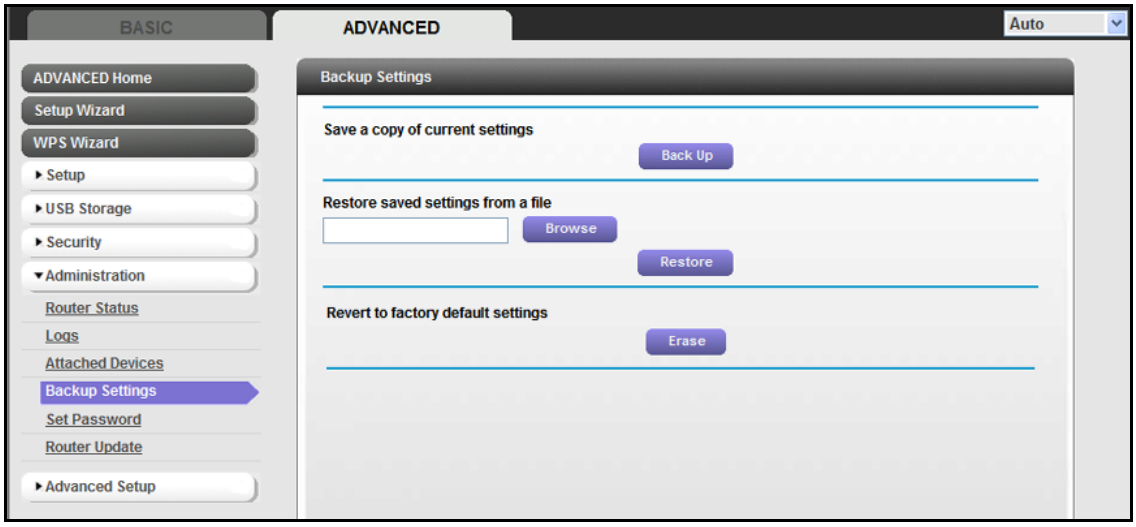
Manage the Configuration File

The configuration settings of the N600 Wireless Dual Band 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.

Backup Settings

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

1. Select **Advanced > Administration > BackUp Settings** to display the following screen:



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

Restore Configuration Settings

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

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

Upon completion, the router reboots.

WARNING!

Do not interrupt the reboot process.

Erase

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

You can either use the Restore Factory Settings button on the back of the router (see *Factory Settings* on page 110), or you can click the **Erase** button in this screen.

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

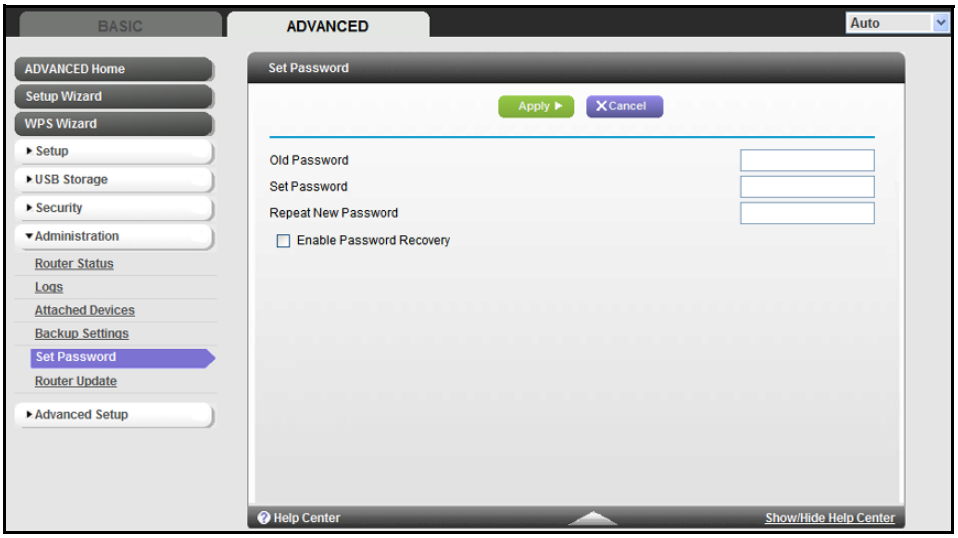
Set Password

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

This 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 14).

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

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



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

Password Recovery

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

➢ **To set up password recovery:**

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

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

Advanced Settings

8

Fine tuning your network

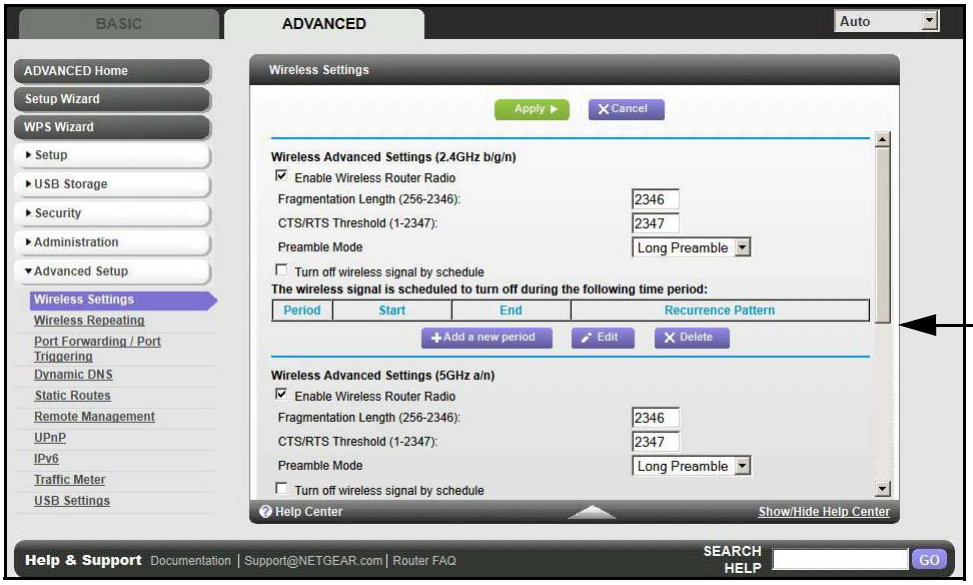
This chapter describes the advanced features of your router. The information is for users with a solid understanding of networking concepts who want to set the router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter includes the following sections:

- *Advanced Wireless Settings*
- *Wireless Repeating Function (WDS)*
- *Port Forwarding and Triggering*
- *Set up Port Forwarding to Local Servers*
- *Set up Port Triggering*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *USB Settings*
- *Universal Plug and Play*
- *IPv6*
- *Traffic Meter*

Advanced Wireless Settings

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



The following settings are available in this screen:

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

> **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.

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

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

AP Mode. You can make the WNDR3400v2 function as an access point.

Wireless Card Access List. Click the **Set Up Access List** button display the Wireless Card Access List screen. On this screen, you can restrict access to your network to specific devices based on their MAC address.

Wireless Repeating Function (WDS)

You can set the N600 Wireless Dual Band Router up to be used as a wireless access point (AP). This enables the router to act as a wireless repeater. A wireless repeater connects to another wireless router as a client where the network to which it connects becomes the ISP service.

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

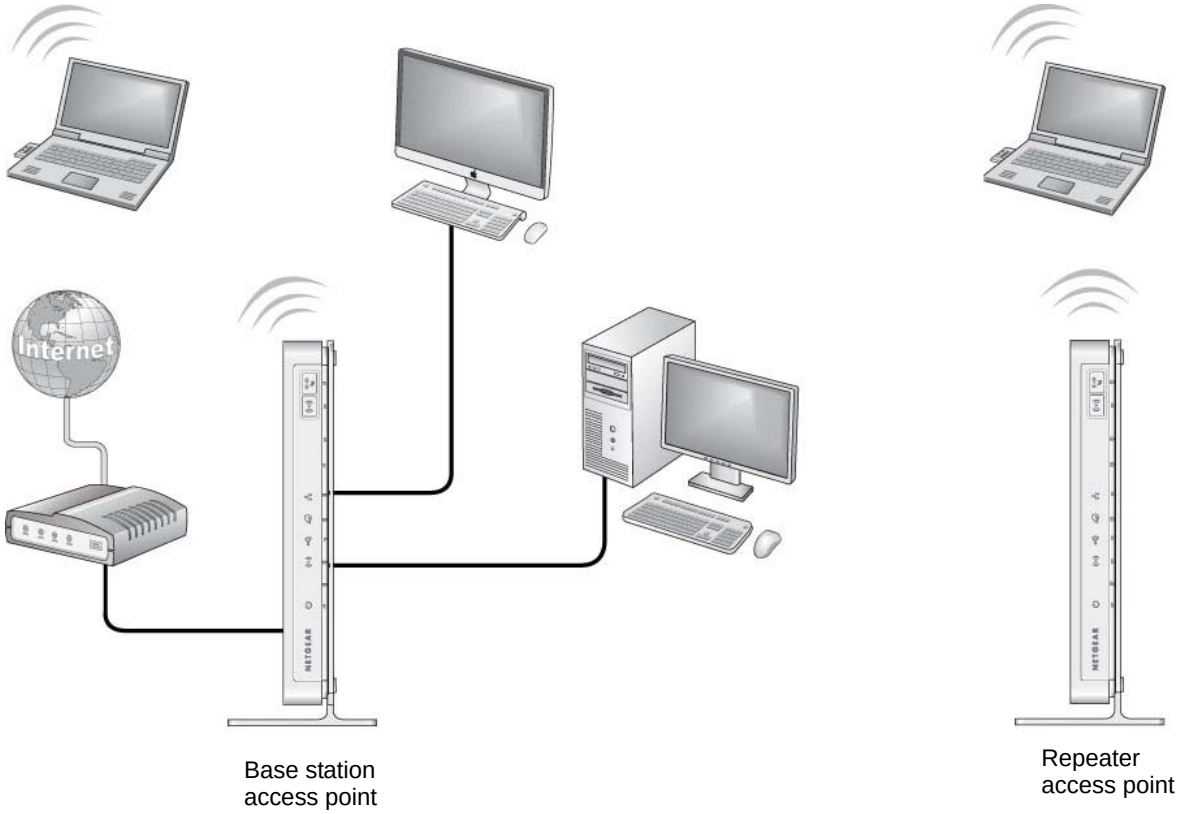


Figure 4. Wireless repeating scenario

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

Wireless Base Station. The router acts as the parent access point, bridging traffic to and from the child repeater access point, as well as handling wireless and wired local computers.

To configure this mode, you have to know the MAC addresses of the child repeater access point.

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

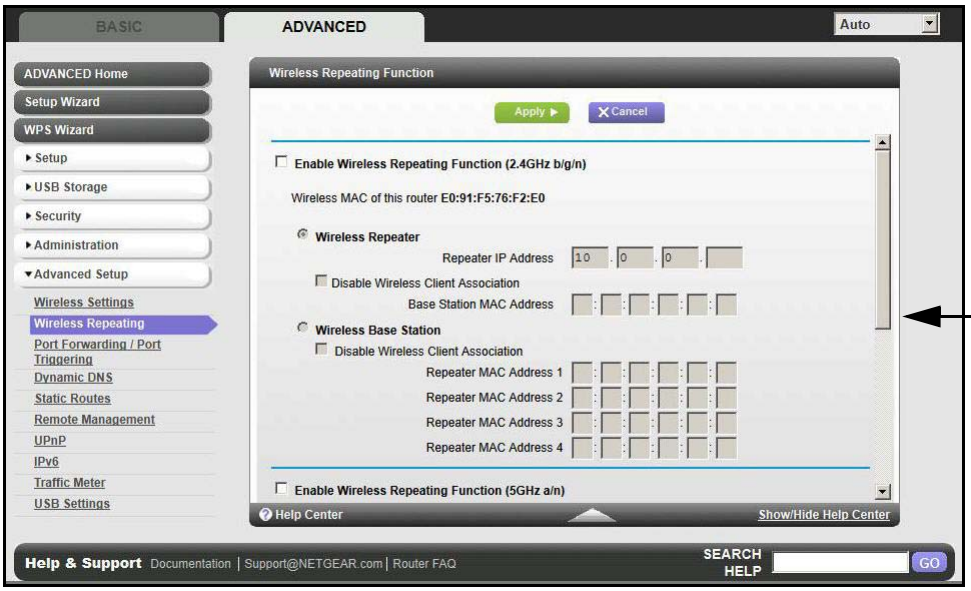
The WNDR3400v2 router is always in dual band concurrent mode, unless you turn off one radio. If you enable the wireless repeater in either radio band, the wireless base station, or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either 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, the following conditions have to be met for both access points:

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

Wireless Repeating Function

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



- **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 this check box.
  - If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

  Base Station MAC Address. If your router is the repeater, enter the MAC address for the access point that is the base station.
- **Wireless Base Station**. If your router is the base station, select this 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 four other access points. Enter the MAC addresses of the other access points in these fields.

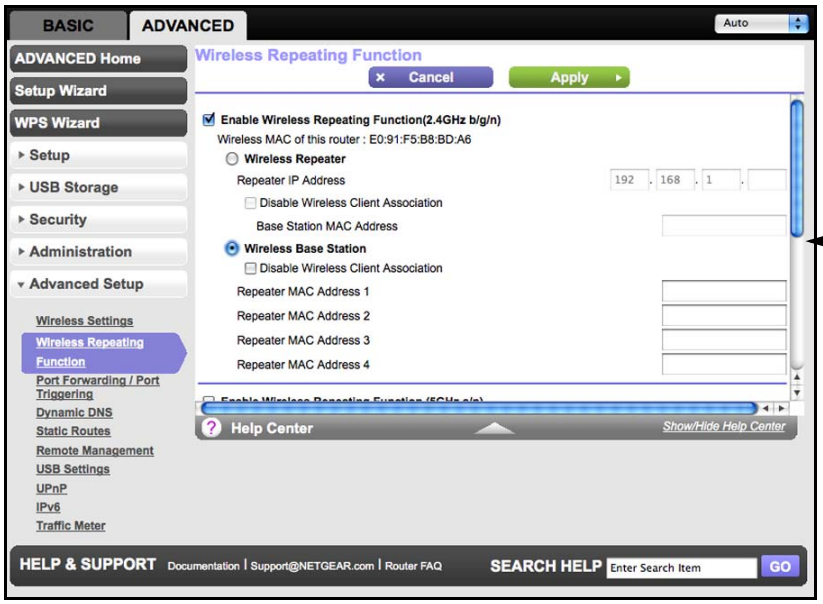
Set up the Base Station

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

➢ **To set up the base station:**

1. Set up both units with the same wireless settings (SSID, mode, channel, and security). The wireless security option has to be set to None or WEP.

2. Select **Advanced > Advanced Setup > Wireless Repeating Function** to display the Wireless Repeating Function screen.



3. In the Wireless Repeating Function screen (depending on the frequency you want to use), select the **Enable Wireless Repeating Function** check box and select the **Wireless Base Station** radio button.
4. Enter the MAC address for one or more repeater units.
5. Click **Apply** to save your changes.

Set up a Repeater Unit

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

> **Note:** If you are using the WNDR3400v2 base station with a non-NETGEAR router as the repeater, you might need to change more configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

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

1. Log in to the router that will be the repeater. Select **Basic > Wireless Settings** and verify that the wireless settings match the base unit exactly. The wireless security option has to be set to **WEP** or **None**.
2. Select **Advanced > Wireless Repeating Function**, and select the **Enable Wireless Repeating Function** check box and the **Wireless Repeater** radio button.
3. Fill in the Repeater IP Address field. This IP address has to be in the same subnet as the base station, but different from the LAN IP of the base station.

4. Click **Apply** to save your changes.
5. Verify connectivity across the LANs.

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

Port Forwarding and Triggering

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

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

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

Remote Computer Access Basics

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

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

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

   Source address. Your computer's IP address.

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

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

   Destination port number. 80, which is the standard port number for a web server process.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at www.example.com. Before sending the web page request message to www.example.com, your router stores the original

information and then modifies the source information in the request message, performing Network Address Translation (NAT):

- The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
- The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

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

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

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

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

   Destination address. The public IP address of your router.

   Destination port number. 33333.

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

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

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

   Destination address. Your computer's IP address.

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

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

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply to a different port number, your router does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies to multiple port numbers. Using the port triggering function of your router, you can tell the router to open 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 have to also allow incoming traffic on port 113 to reach the originating computer.” Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, say port 33333) as the destination port. The IRC server also sends an identify message to your router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether 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 triggers the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

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

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the

Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

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

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

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

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

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

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

   The destination address is replaced with 192.168.1.123.

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

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

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

How Port Forwarding Differs from Port Triggering

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

- Port triggering is 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 requires that you know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Set up Port Forwarding to Local Servers

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

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

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

➢ **To set up port forwarding:**

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your N600 Wireless Dual Band Router.

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

Port Forwarding is selected as the service type.

2. From the Service Name list, select the service or game that you will host on your network. If the service does not appear in the list, see *Add a Custom Service* on page 87.
3. In the corresponding Server IP Address field, enter the last digit of the IP address of your local computer that provides this service.
4. Click **Add**. The service appears in the list in the screen.

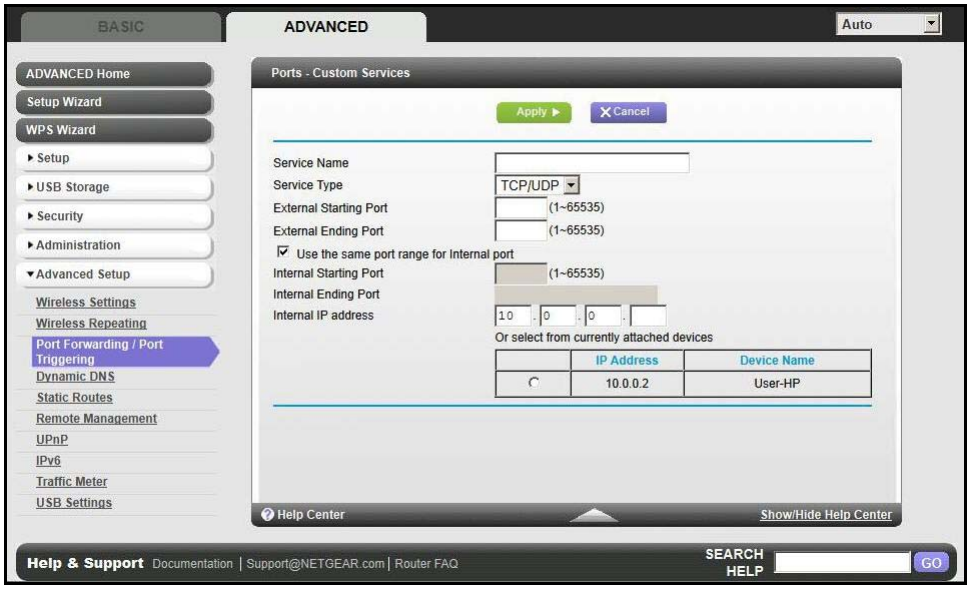
Add a Custom Service

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

➢ **To add a custom service:**

1. Select **Advanced > Advanced Setup > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.

3. Click the **Add Custom Service** button to display the following screen:



4. In the Service Name field, enter a descriptive name.
5. In the Protocol list, select the protocol. If you are unsure, select **TCP/UDP**.
6. In the Starting Port field, enter the beginning port number.
   - If the application uses a single port, enter the same port number in the Ending Port field.
   - If the application uses a range of ports, enter the ending port number of the range in the Ending Port field.
7. In the Server IP Address field, enter the IP address of your local computer that provides this service.
8. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Editing or Deleting a Port Forwarding Entry

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

1. In the table, select the radio button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Making a Local Web Server Public

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

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

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation. In this example, your router always gives your web server an IP address of 192.168.1.33.

2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your web server at **192.168.1.33**. HTTP (port 80) is the standard protocol for web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name as described in *Dynamic DNS* on page 91. To access your web server from the Internet, a remote user has to know the IP address assigned by your ISP. 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.

While 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.

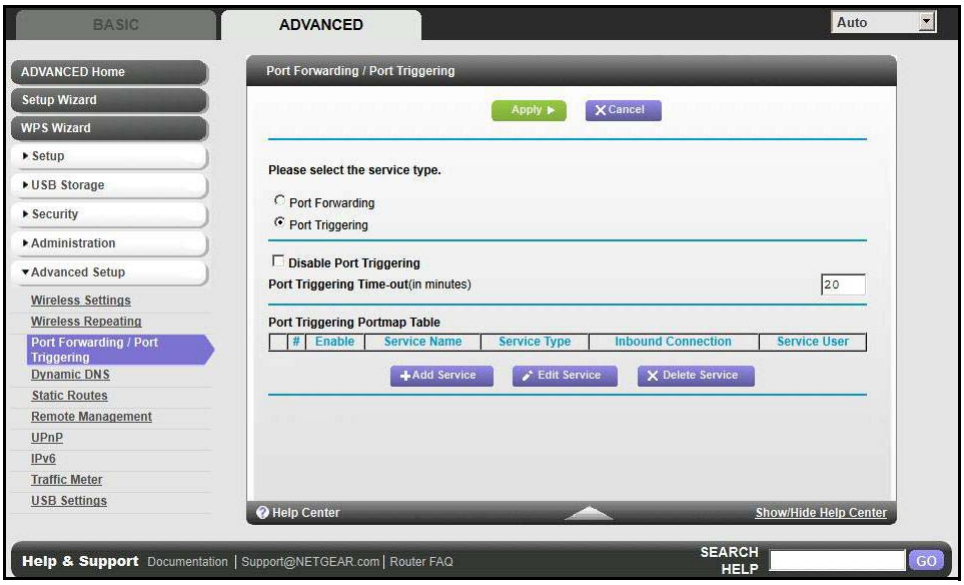
Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 96.

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

➢ **To set up port triggering:**

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

2. Select the **Port Triggering** radio button to display the port triggering information.

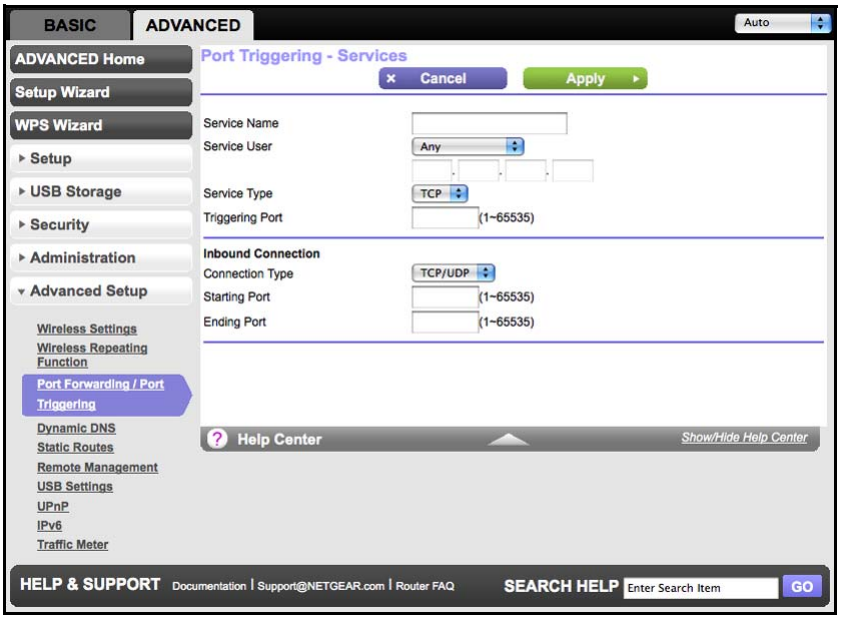


3. Clear the **Disable Port Triggering** check box if it is selected.

   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.
5. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

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



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

Dynamic DNS

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

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

Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. First visit their website at *http://www.dyndns.org* and obtain an account and

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

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

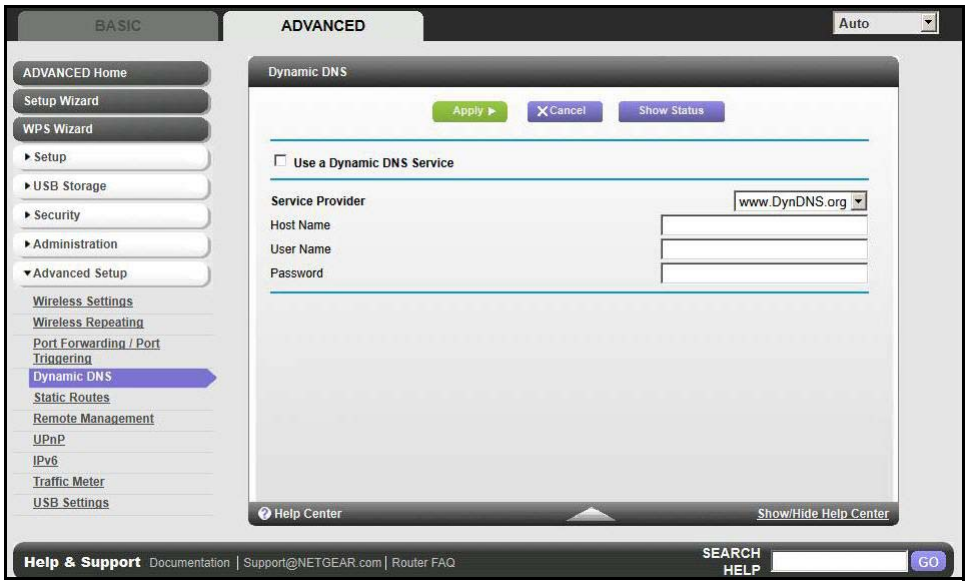


Figure 5. Forward traffic to a changing IP address

➢ **To set up Dynamic DNS:**

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

   For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
8. Click **Apply** to save your configuration.

Static Routes

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

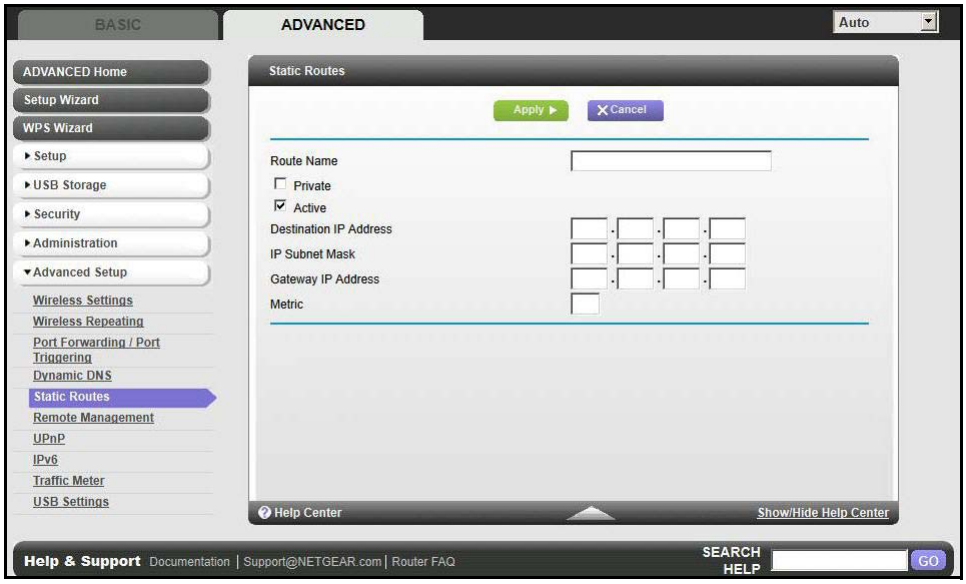
When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 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 have to define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. In this example:

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

➢ **To set up a static route:**

1. Select **Advanced > Advanced Setup > Static Routes**, and click **Add** to display the following screen:



2. In the Route Name field, type a name for this static route (for identification purposes only.)
3. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.
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, which has to be a router on the same LAN segment as the N600 Wireless Dual Band Router.
8. Type a number between 1 and 15 as the metric value.

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

Remote Management

The remote management feature lets you upgrade or check the status of your N600 Wireless Dual Band Router over the Internet.

➢ **To set up remote management:**

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

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

2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, specify the external IP addresses allowed to access the router's remote management.

__Note:__ For enhanced security, restrict access to as few external IP addresses as practical.

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that is allowed access.
- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.
- To allow access from any IP address on the Internet, select **Everyone**.

4. Specify the port number for accessing the 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 between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click **Apply** to have your changes take effect.
6. When accessing your router from the Internet, type your router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter **http://134.177.0.123:8080** in your browser.

USB Settings

For added security, the router can be set up to share only approved USB devices. See *Specify Approved USB Devices* on page 56 for the procedure.

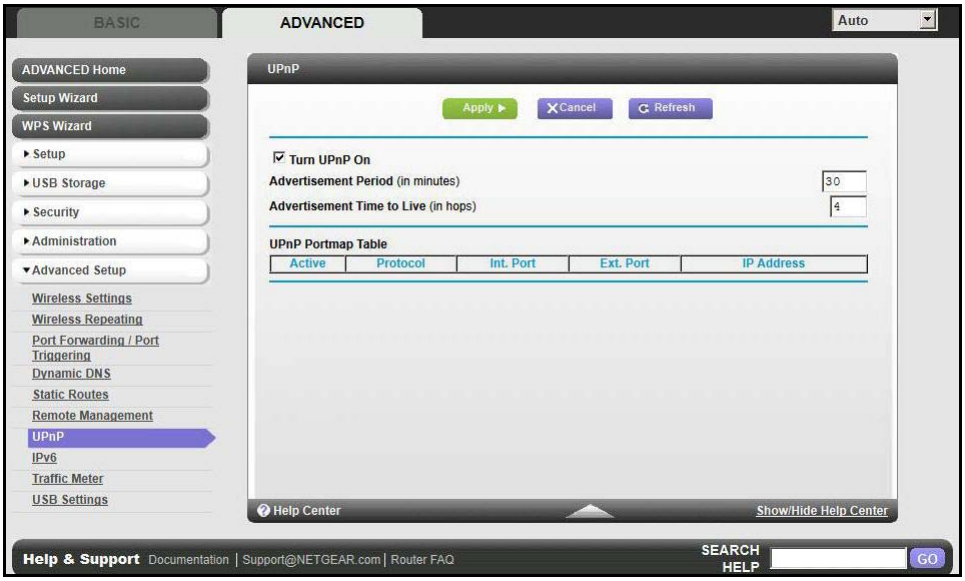
Universal Plug and Play

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

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

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

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



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

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

   Advertisement Period. The advertisement period is how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of 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 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, it might be necessary to increase this value.

   UPnP Portmap Table. The UPnP Portmap Table displays the IP address of each UPnP device that is 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.

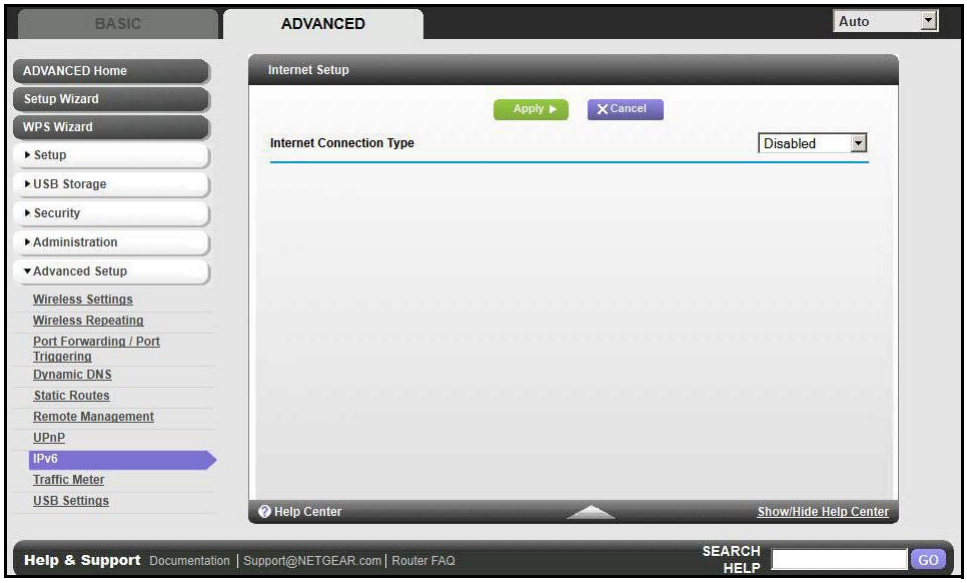
3. Click **Apply** to save your settings.

IPv6

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

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

1. Select **Advanced > Advanced Setup > IPv6** to display the following screen:



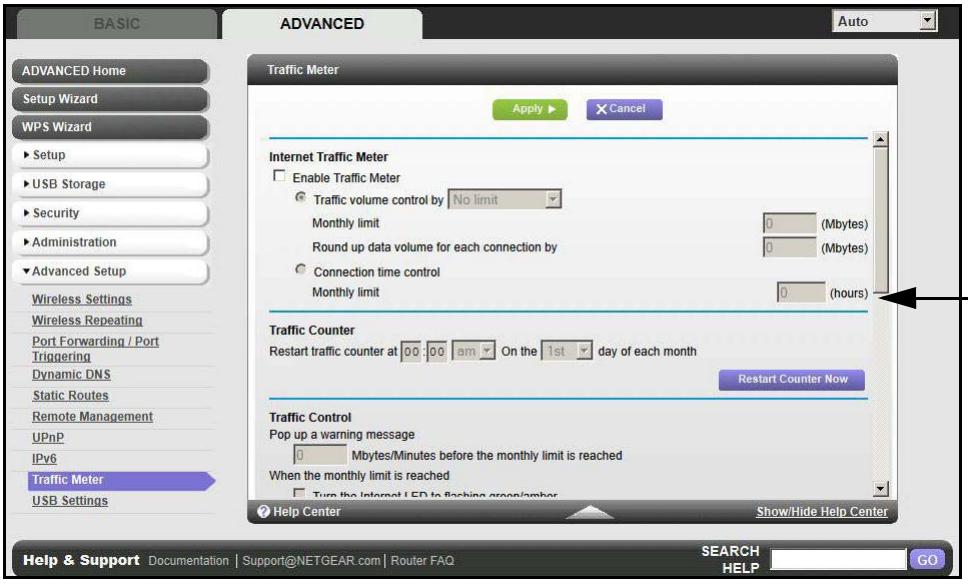
2. Select the IPv6 connection type from the list. Your Internet service provider (ISP) can provide this information.
   - If your ISP did not provide details, you can select **IPv6 Tunnel**.
   - If you are not sure, select **Auto Detect** so that the router detects the IPv6 type that is in use.
   - If your Internet connection does not use PPPoE, DHCP, or fixed, but is IPv6, select **IPv6 Auto Config**.
3. Click **Appl**y so that your changes take effect.

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** to display the following screen:



Scroll to view more settings

2. To enable the Traffic Meter, select the **Enable Traffic Meter** check box.
3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:
   - **No Limit**. No restriction is applied when the traffic limit is reached.
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
4. You can limit the amount of data traffic allowed per month by specifying how many Mbytes per month are allowed or by specifying how many hours of traffic are allowed.
5. Set the Traffic Counter to begin at a specific time and date.
6. Set up Traffic Control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   - The Internet LED flashes green or amber.
   - The Internet connection is disconnected and disabled.
7. Set up Internet Traffic Statistics to monitor the data traffic.
8. Click the **Traffic Status** button to get a live update on Internet traffic status on your router.
9. Click **Apply** to save your settings.

Troubleshooting

9

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

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshooting with the LEDs*
- *Cannot Log in to the Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *Incorrect Date or Time*
- *Wireless Connectivity*
- *Restore the Factory Settings and Password*
- *Troubleshoot Your Network Using the Ping Utility*

Quick Tips

This section describes tips for troubleshooting some common problems.

Sequence to Restart Your Network

Be sure to restart your network in this sequence:

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

Check Ethernet Cable Connections

Make sure that the Ethernet cables are securely plugged in:

- The Internet status LED on the router is on if the Ethernet cable connecting the router and the modem is plugged in securely and the modem and router are turned on.
- For each powered-on computer connected to the router by an Ethernet cable, the corresponding numbered router LAN port LED is on.

Wireless Settings

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

- For a wirelessly connected computer, the wireless network name (SSID) and wireless security settings of the router and wireless computer need to match exactly.
- If you set up an access list in the Advanced Wireless Settings screen, you have to add each wireless computer’s MAC address to the router’s access list.

Network Settings

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

- Wired and wirelessly connected computers need to have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen.

Troubleshooting with the LEDs

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

1. When power is first applied, verify that the Power/Test LED is on.
2. Verify that the Power/Test LED turns amber within a few seconds, indicating that the self-test is running.
3. After approximately 30 seconds, verify that:
   - The Power/Test LED is solid green.
   - The Internet LED is lit.
   - A numbered Ethernet port LED is on for any local port that is connected to a computer. This 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/Test LED Is Off or Blinking

- Make sure that the power cord is securely connected to your router and that the power adapter is securely connected to a functioning power outlet.
- Make sure that you are using the power adapter that NETGEAR supplied for this product.
- If the Power/Test LED blinks slowly and continuously, the router firmware is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. If the error persists, you have a hardware problem. For recovery instructions or help with a hardware problem, contact technical support at http://support.netgear.com/general/contact/default.aspx.

Power/Test LED Stays Amber

When the router is turned on, the Power/Test LED turns amber for about 20 seconds and then turns green. If the LED does not turn green, the router has a problem.

If the Power/Test LED is still amber 1 minute after turning on power to the router:

1. Turn the power off and back on to see if the router recovers.
2. Press and hold the **Restore Factory Settings** button to return the router to its factory settings. See *Factory Settings* on page 110.

If the error persists, you might have a hardware problem and should contact technical support at *www.netgear.com/support*.

LEDs Never Turn Off

When the router is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the router.

If all LEDs are still on 1 minute after power-up:

- Cycle the power to see if the router recovers.
- Press and hold the **Restore Factory Settings** button to return the router to its factory settings. See *Factory Settings* on page 110.

If the error persists, you might have a hardware problem and should contact technical support at *www.netgear.com/support*.

Internet or Ethernet Port LEDs Are Off

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

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

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

Wireless LEDs Are Off

If the Wireless LEDs stay off, check to see if the Wireless On/Off button on the router has been pressed. This button turns the wireless radios in the router on and off. The Wireless LEDs are lit when the wireless radio is turned on.

The Push 'N' Connect (WPS) Button Blinks Amber

If, after using the WPS function, the button blinks amber, check the following:

- Make sure that you are using the button and not the router's built-in registrar.
- Check that PIN verification succeeded for the wireless device that you are adding to the wireless network.
- Make sure that you have not pressed the WPS button on the top of the router after disabling the WPS feature (you logged in to the router and disabled this previously).
- Check that the router is not in the temporary AP setup locked state (if you are using the wireless repeater function).

Cannot Log in to the Router

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous 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 MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These autogenerated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. This procedure is explained in *Factory Settings* on page 110.
- 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 instead. NETGEAR does not support such a configuration.
- If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services, for example, converting ADSL or cable data into Ethernet networking information. NETGEAR does not support such a configuration.

Cannot Access the Internet

If you can access your router but you are unable to access the Internet, first determine whether the router can obtain an IP address from your Internet service provider (ISP). Unless your ISP provides a fixed IP address, your router requests an IP address from the ISP. You can determine whether the request was successful using the Router Status screen.

➢ **To check the WAN IP address:**

1. Start your browser and select an external site such as *http://www.netgear.com*.
2. Access the router interface at *http://www.routerlogin.net*.
3. Select **Administration > Router Status**.
4. Check that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network, as described in *Sequence to Restart Your Network* on page 101.

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

- Your Internet service provider (ISP) might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Internet 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.

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

- Your computer might not recognize any DNS server addresses.

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

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

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

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

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

Troubleshooting PPPoE

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

➢ **To troubleshoot a PPPoE connection:**

1. Log in to the router.
2. Select **Administration > Router Status**.
3. Click **Connection Status**. If all of the steps indicate OK, your PPPoE connection is working.

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

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

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

Troubleshooting Internet Browsing

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

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

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

  Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.
- Your computer might not have the router configured as its default gateway.

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

  If the router does not save changes you have made in the browser interface, check the following:
- When entering configuration settings, be sure to click **Apply** before moving to another screen or tab, or your changes could be lost.
- Click **Refresh** or **Reload** in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

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.

Incorrect Date or Time

Select **Advanced > Security > Schedule** to display the current date and time. The router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000. This means the router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have finished setting up the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour. The router does not automatically sense daylight savings time. In the Schedule screen, select the **Automatically adjust for daylight savings time** check box.

Wireless Connectivity

If you are having trouble connecting wirelessly to the router, try to isolate the problem.

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

  If not, check the Wireless LEDs on the front of the router. They should be lit. If they are not, you can press the **WiFi On/Off** button on the back of the router to turn the router's wireless radio back on.

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

- Does your wireless device support the security that you are using for your wireless network (WPA or WPA2)?
- If you want to view the wireless settings for the router, use an Ethernet cable to connect a computer to a LAN port on the router. Then log in to the router and select **Setup > Wireless Settings** see (*Basic Wireless Settings* on page 27).

  Note: *Be sure to click **Apply** if you make changes.*

Wireless Signal Strength

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 away, and see whether the signal strength improves.
- Is your wireless signal blocked by objects between the router and your computer?

Restore the Factory Settings and Password

This section explains how to restore the factory settings, changing the router's administration password back to **password**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see *Erase* on page 73).
- Use the Restore Factory Settings button on the back of the router. See *Factory Settings* on page 110. If you restore the factory settings and the router fails to restart, or the green Power/Test LED continues to blink, the unit might be defective. If the error persists, you might have a hardware problem and should contact technical support at *http://www.netgear.com/support*.

Troubleshoot Your Network Using the Ping Utility

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

Test the LAN Path to Your Router

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

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

1. From the Windows toolbar, click **Start**, and then 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 on for the port to which you are connected.

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

- Wrong network configuration

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

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

Test the Path from Your Computer to a Remote Device

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

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

   ping -n 10 <*IP address*>

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

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

If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Internet 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, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If so, configure your router to "clone" or "spoof" the MAC address from the authorized computer.

Supplemental Information

A

This appendix provides factory default settings and technical specifications for the N600 Wireless Dual Band Router WNDR3400v2.

Factory Settings

You can return the router to its factory settings. Use the end of a paper clip or some other similar object to press and hold the **Restore Factory Settings** button on the back of the router for at least 5 seconds. The router resets and returns to the factory settings. Your device returns to the factory configuration settings shown in the following table.

Table 4. Factory default settings

Feature		Default behavior
Router login	User login URL	www.routerlogin.com or www.routerlogin.net
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default hardware address
	WAN MTU size	1500
	Port speed	Autosensing
Local network (LAN)	LAN IP	192.168.1.1
	Subnet mask	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	Pacific time
	Time zone daylight saving time	Disabled
	Allow a registrar to configure this router	Enabled

Table 4. Factory default settings (continued)

Feature		Default behavior
Local network (LAN) continued	DHCP starting IP address	192.168.1.2
	DHCP ending IP address	192.168.1.254
	DMZ	Disabled
	Time zone	GMT for WW except NA and GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless	Wireless communication	Enabled
	SSID name	See router label
	Security	Enabled
	Broadcast SSID	Enabled
	Transmission speed	Auto*
	Country/region	United States in the US, otherwise varies by region
	RF channel	6 until region selected
	Operating mode	Up to 300 Mbps
	Data rate	Best
	Output power	Full
Firewall	Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests)
	Outbound (communications going out to the Internet)	Enabled (all)

**. Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will 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 5. WNDR3400v2 Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power adapter	• North America: 120V, 60 Hz, input • UK, Australia: 240V, 50 Hz, input • Europe: 230V, 50 Hz, input • All regions (output): 12V DC @ 2.5A, output
Dimensions	8.8 in. x 6.8 in. x 1.2 in. (223 x 153 x 31 mm)
Weight	1.2 lbs. (0.5 kg)
Operating temperature	0° to 40° C (32º to 104ºF)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	FCC Part 15 Class B VCCI Class B EN 55 022 (CISPR 22), Class B C-Tick N10947
LAN	10BASE-T or 100BASE-TX, 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 802.11n version 2.0 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b 2.4 GHz IEEE 802.11n, IEEE 802.11a 5.0 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).

Table 5. WNDR3400v2 Router specifications (continued)

Feature	Description
Operating frequency range	2.4 GHz 2.412–2.462 GHz (US) 2.412–2.472 GHz (Japan) 2.412–2.472 GHz (Europe ETSI) 5 GHz 5.18–5.24 + 5.745–5.825 GHz (US) 5.18–5.24 GHz (Europe ETSI) FCC: 5.25–5.35 GHz (DFS band) 5.47–5.725 GHz (DFS band) 5600–5650 MHz is disabled and unavailable for use CE (Europe ETSI): 5.25–5.35 GHz (DFS band) 5.47–5.725 GHz (DFS band)
802.11 security	WPA-PSK, WPA2-PSK, and WPA/WPA2 Enterprise.

Notification of Compliance

B

NETGEAR Dual Band - Wireless

Regulatory Compliance Information

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

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

Europe – EU Declaration of Conformity

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

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

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

- R&TTE Directive 1999/5/EC

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

Intended for indoor use only in all EU member states, EFTA states, and Switzerland.

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

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N600 Wireless Dual Band Router WNDR3400v2 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

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

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

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N600 Wireless Dual Band Router WNDR3400v2) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

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

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

Industry Canada

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

IMPORTANT NOTE: Radiation Exposure Statement:

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

Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce po-tential for harmful interference to co-channel mobile satellite systems.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

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

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

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

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utili-sation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

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

A

access
- remote 95
- viewing logs 71

access points 78

accessing remote computer 82

adding
- custom services 87
- guest network 31
- priority rules 45
- QoS policy 44
- wireless devices 21

address reservation 43

advertisement period 97

alerts, emailing 63

applications, QoS for online gaming 45

approved USB devices 56

attached devices 25

authentication, required by mail server 64

automatic firmware checking 66

automatic Internet connection 35

B

back panel 13

backing up configuration 73

base station, setting up 80

blocking
- inbound traffic 82
- keywords 60
- services 61
- sites 60

box contents 8

C

cables, checking 101

changes not saved, router 106

compliance 114

configuration file 72, 73

configuring
- DMZ server 39
- Dynamic DNS 92
- NAT 38
- port forwarding 86
- port triggering 89
- QoS 44
- repeater unit 81
- user-defined services 61

connecting wirelessly 8

country setting 35

crossover cable 103

CTS/RTS Threshold 77

custom service (port forwarding) 87

D

dashboard 20

data packets, fragmented 39

date and time 107

daylight savings time 107

default DMZ server 39

default factory settings 73, 110

default gateway 69

deleting
- configuration 73
- keywords 60
- port forwarding entry 88
- QoS policy 48

denial of service (DoS) protection 59

devices, attached 25

DHCP server 42, 69

DHCP setting 68

DMZ server 39

DNS addresses
- primary 24
- troubleshooting 105

DNS servers 82

Domain Name Server (DNS) addresses 24, 68

Dynamic DNS 91

E

electromagnetic emissions 112

email notices 63

erasing configuration 73

Ethernet cables, checking 101
Ethernet LED, troubleshooting 102, 103

F

factory default settings
  list of 110
  restoring 73
file sharing 51
firmware version 67
firmware, upgrading 19, 66
fragmentation length 77
fragmented data packets 39
front panel 11

G

games, online, QoS for 45
gateway IP address 24
Genie, NETGEAR
  settings, advanced 34
  settings, basic 22
  setup, initial 18
  using, after installation 19
guest networks 31, 71

H

host name 23
host, trusted 60

I

inbound traffic, allowing or blocking 82
installing 18, 35
Internet connection
  setting up 23
  troubleshooting 104
Internet LEDs, troubleshooting 102
Internet port 35, 67
Internet Relay Chat (IRC) 84
Internet service provider (ISP)
  account information 17
  Internet Setup screen fields 23
Internet services, blocking access 61
interval, poll 68
IP addresses
  current 67
  DHCP 17
  dynamic 91
  reserved 43
IP subnet mask 68

K

keywords 60

L

label, product 14
LAN port
  QoS for 46
  settings 67
LAN setup 41
language setting 35
large files, sharing 52
lease, DHCP 69
LEDs
  troubleshooting 102
  verifying cabling 15
local servers, port forwarding to 86
logging in 17, 19
logs
  emailing 63
  viewing 71

M

MAC addresses
  current 67
  product label 14
  QoS for 47
mail server, outgoing 64
maintenance settings 65
managing router remotely 95
menus, described 20
metric value 94
mixed mode security options 33
MTU size 39
multicasting 42

N

NAT (Network Address Translation) 38, 83
NETGEAR Genie
  settings, advanced 34
  settings, basic, initial 22
  setup, initial 18
  using, after installation 19
Network Time Protocol (NTP) 107
network, correct settings, checking 101
network, restarting 101
networks, guest 31, 71

O

outgoing mail server 64

P

packets, fragmented 39
Parental Controls 26
passphrases
  changing 30
  product label 14
password recovery, admin 74
password, restoring 108
photos, sharing 51
poll interval 68
port filtering 61
port forwarding 82, 84, 85, 86
port numbers 61
port status 68
port triggering 82, 83, 85, 89
ports, listed, back panel 13
positioning the router 8
Power LED, troubleshooting 102
PPPoE (PPP over Ethernet) 105
Preamble mode 77
preset security
  about 27
  passphrase 30
primary DNS addresses 24
printing files and photos 51
prioritizing traffic 44
Push 'N' Connect 21

Q

QoS (Quality of Service) 44

R

radio, wireless 77
range of wireless connections 8
ReadyShare access 50, 53
recovering admin password 74
releasing connection status 69
remote management 95
renewing connection status 69
repeater units 81
reserved IP adresses 43
restarting network 101
restoring
  configuration file 73
  default factory settings 13, 108
router interface, described 20
router status, viewing 67

S

scheduling keyword and service blocking 63
secondary DNS 24
security 27
  firewall settings 59
  see also security options
security options 32
security PIN 14, 36
sending logs by email 63
serial number, product label 14
services, blocking 61
settings, default. *See* default factory settings
Setup Wizard 35
sharing files 51
sites, blocking 60
SMTP server 64
specifications, technical 110
SSID
  described 29
  product label 14
static routes 93
status, router, viewing 67
subnet mask 68
system up time 68

T

technical specifications 110
Temporal Key Integrity Protocol (TKIP) 32
time of day 107
time to live, advertisement 97
time-out, port triggering 90
traffic metering 98
troubleshooting 100
  date or time incorrect 107
  log in access 103
  router changes not saved 106
trusted host 60

U

Universal Plug and Play (UPnP) 96
up time, system 68
upgrading firmware 19, 66
USB
  advanced configuration 54

basic storage settings 52
drive requirements 50
file sharing 51
ReadyShare access 50, 53
remote computer connection 57
specifying approved devices 56
unmounting a USB drive 56
USB devices, approved 56
user-defined services 61

V

viewing
logs 71
router status 67

W

WAN IP address, troubleshooting 104
WAN setup 38
WiFi Protected Setup (WPS) 21, 36
wireless channel 29
wireless connections
range 8
troubleshooting 107
wireless devices, adding to the network 21
Wireless Distribution System (WDS) 78, 79
Wireless LEDs, troubleshooting 103, 104
wireless mode 29
wireless network name (SSID)
broadcasting 29
described 29
product label 14
wireless network settings 29
wireless radio 77
wireless repeating 78, 79
base station 80
repeater unit 81
wireless security options 32
Wireless Settings screen 27, 71
checking for correct 101
SSID broadcast 29
WMM (Wi-Fi Multimedia) 44
WPA encryption 32
WPA2 encryption 32
WPA2-PSK encryption 33
WPA-PSK encryption 32
WPA-PSK/WPA2-PSK mixed mode 33
WPS button 21
WPS-PSK encryption 33
WPS-PSK+ WPA2-PSK encryption 33
wrong date or time 107