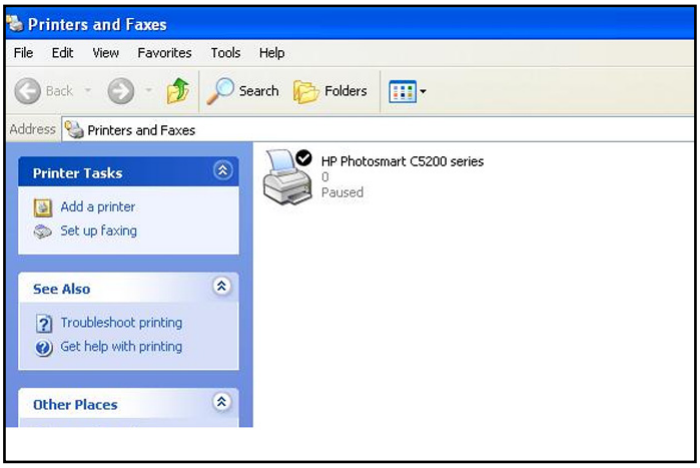
Once the printer shows Available status, it is no longer grayed out in a Paused state in the Windows Printers window.



This USB printer is ready. The utility does not need to always hold the connection of this USB printer. Once there is any print job for this printer, the USB utility connects to this USB printer automatically then prints. After the print job is done, the printer status returns to the Paused state.

Scan with a Multi-Function Printer

You can use the scan feature of a multi-function printer.

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

   This activates the scanner window to perform scans.

USB Speaker

➢ **To control a USB speaker:**

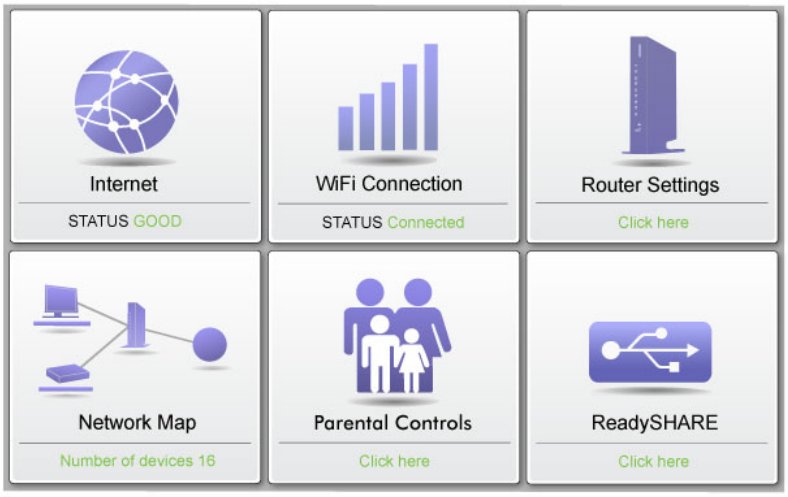
1. Select the USB speaker.
2. Click the **Connect** button to connect this speaker, or click **Disconnect** to disconnect the speaker.

   If you click Connect, and someone else is already connected to the speaker, a request is sent to that person. The person who receives the request can click an Accept or Reject button.

If someone is connected to the speaker and it is not being used (the router does not detect any activity), the router holds the connection for the amount of time that is in the timeout value, and then makes it available.

Desktop NETGEAR genie

Desktop NETGEAR genie is the easy dashboard for managing, monitoring, and repairing your home network.



- Automatically repair common wireless network problems.
- Have easy access to router features like Live Parental Controls, guest access, broadband usage meter, speed test, and more.
- Use the Network map to see all devices on your home network.

To download the free NETGEAR genie, go to this page at the NETGEAR website: *www.NETGEAR.com/genie*.

Security

7

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.

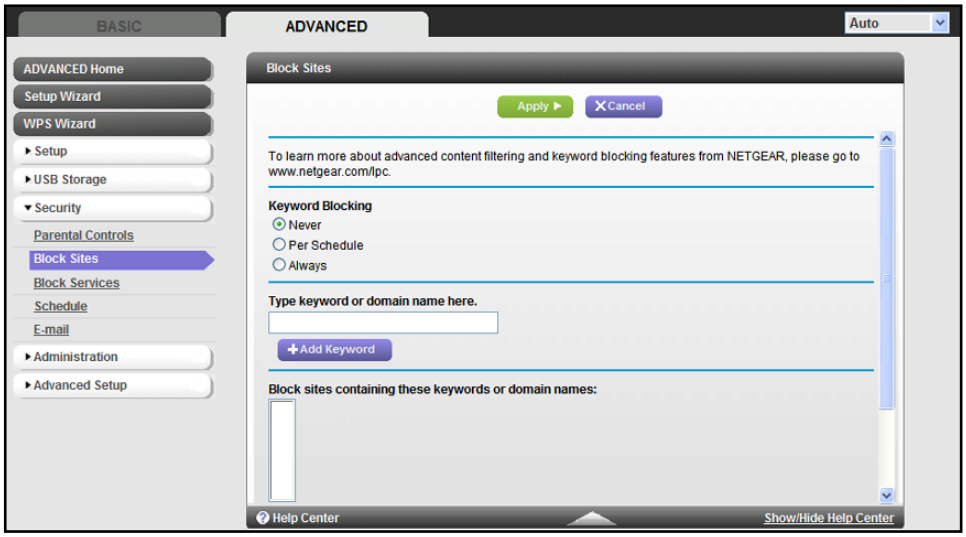
This chapter includes the following sections:

- *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 then **Apply** to save your changes.

➢ **To specify a trusted computer:**

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

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

Block Services (Port Filtering)

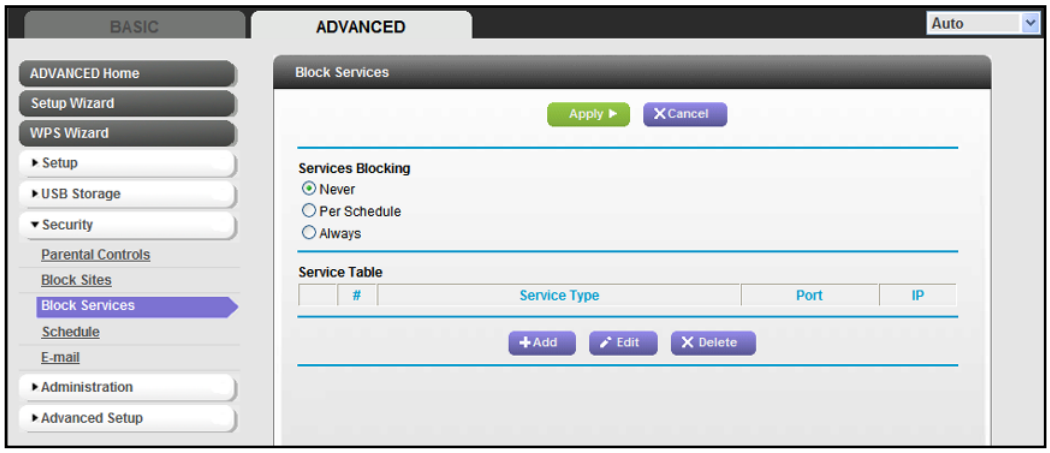
Services are functions performed by server computers at the request of client computers. For example, web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server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

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

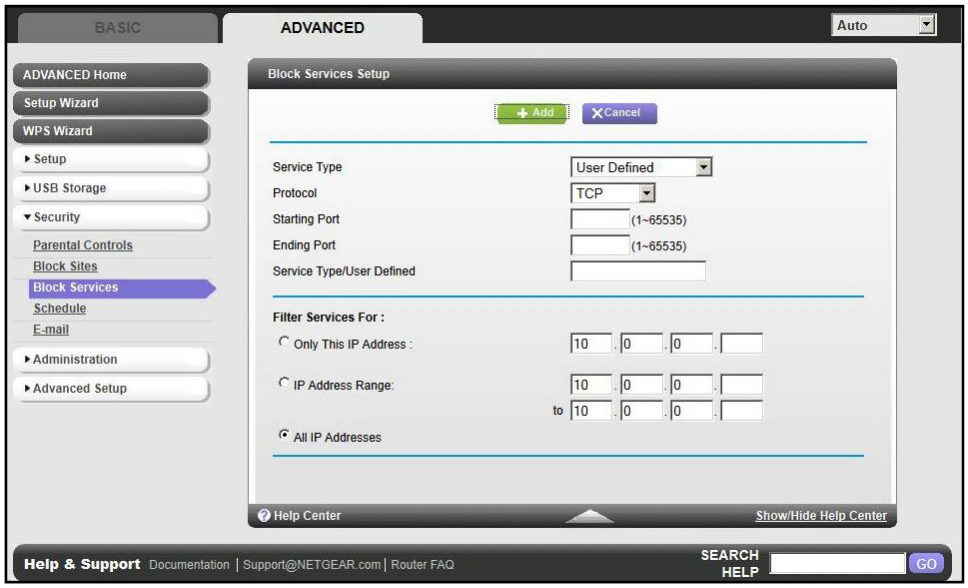
➢ **To block services:**

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 67.

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



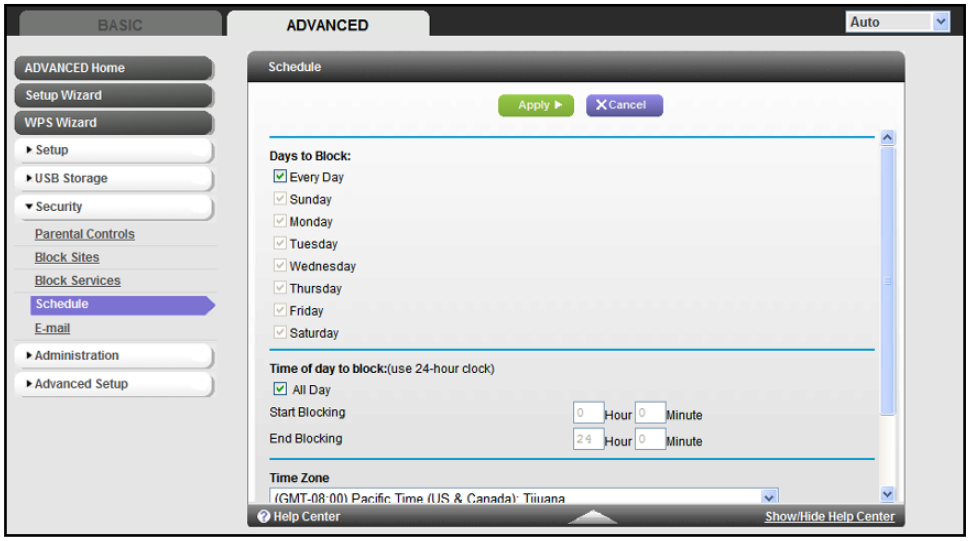
4. From the Service Type list, select the application or service to allow or block. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined.**
5. If you know that the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

Schedule Blocking

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

➢ **To schedule blocking:**

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



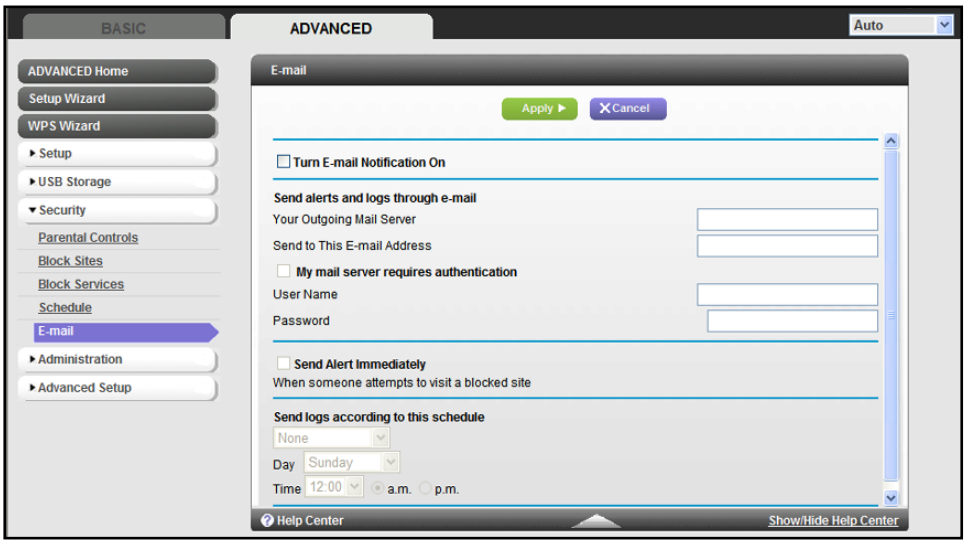
2. Set up the schedule for blocking keywords and services.
   - **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes, or select **Every Day** to select the check boxes for all days.
   - **Time of Day to Block**. Select a start and end time in 24-hour 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

8

Managing your network

This chapter describes the router settings for administering and maintaining your router and home network. See also *Remote Management* on page 105 for information about upgrading or checking the status of your router over the Internet, and *Traffic Meter* on page 109 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*
- *Time Machine*

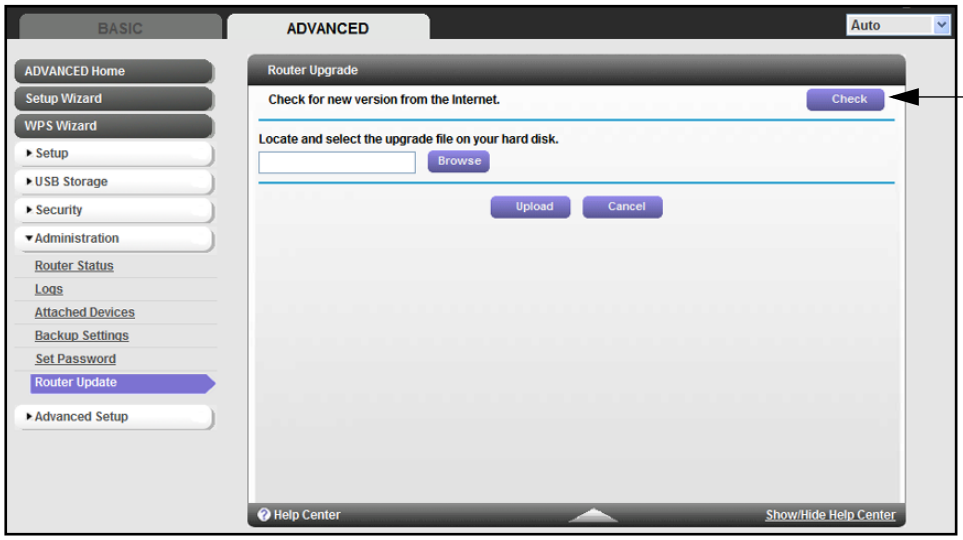
Upgrade the Router Firmware

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

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

➢ **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 information if any is available.

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

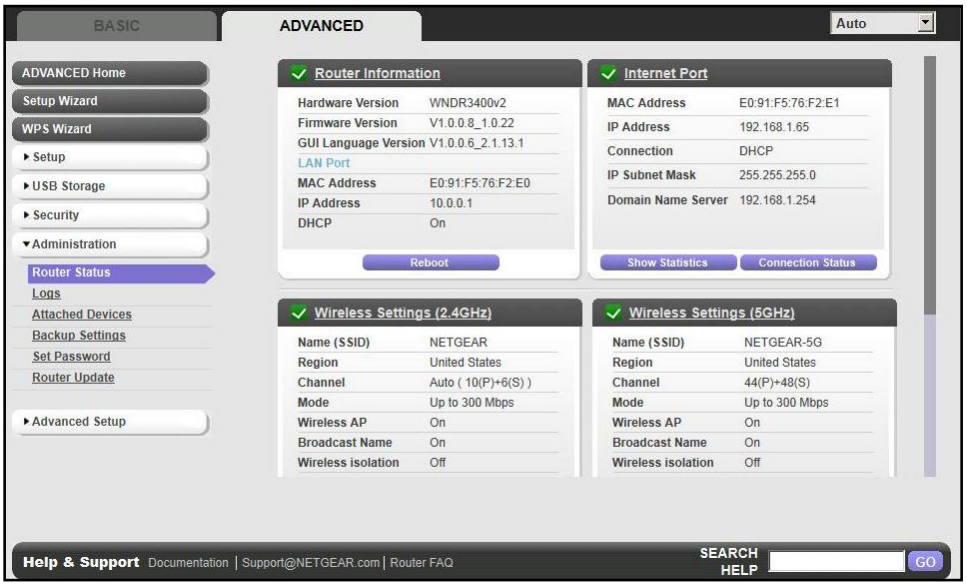
WARNING:

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

When the upload is complete, your router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether or not 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. This is the unique physical address being used by the Ethernet (LAN) port of the router.
- **IP Address**. The IP address being 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. This is the unique physical address being used by the Internet (WAN) port of the router.

IP Address. The IP address being 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 being used by the Internet (WAN) port of the router.

Domain Name Server. The Domain Name Server addresses being 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:

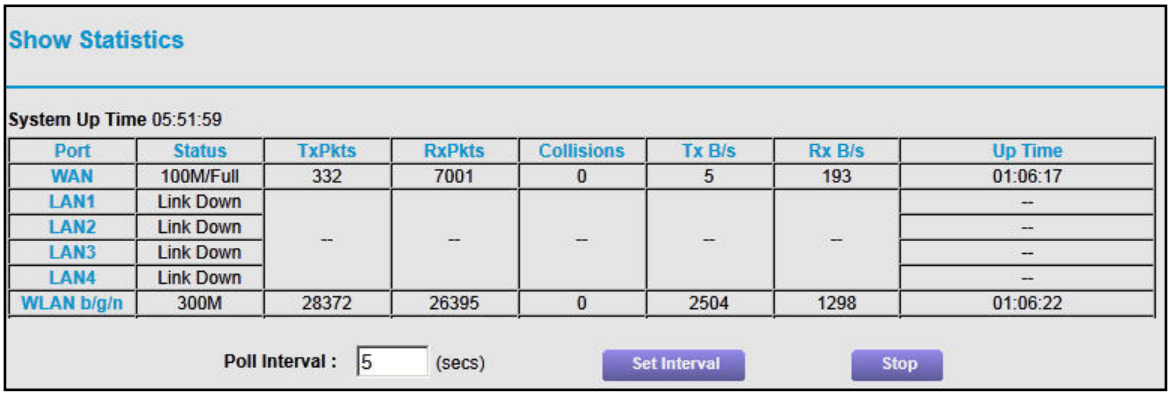


Figure 6. System up time and poll interval statistics

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.

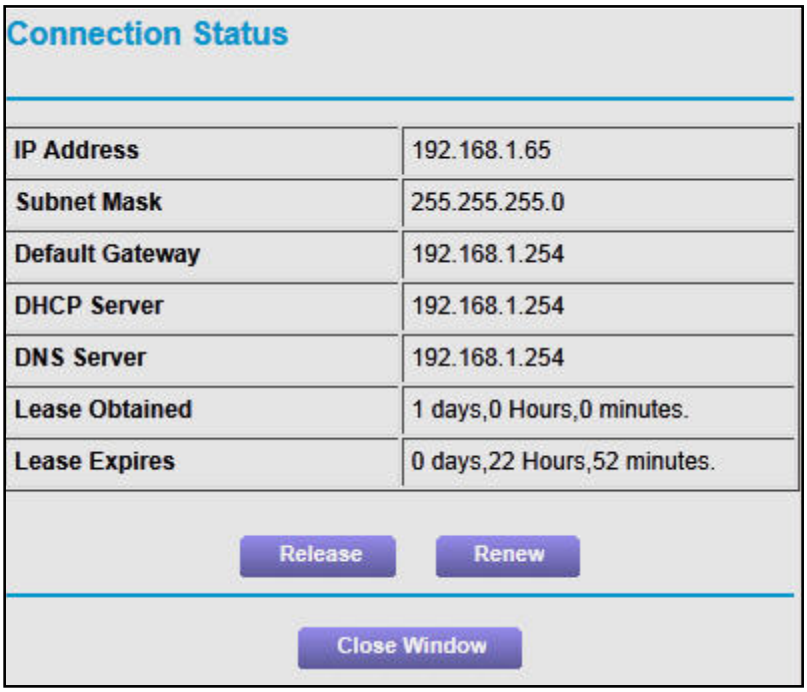


Figure 7. View connection status information

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

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

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

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

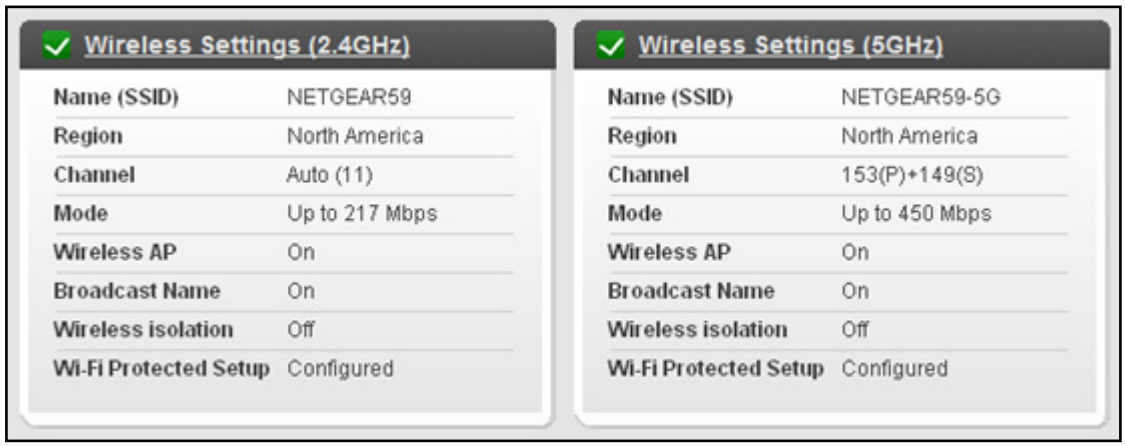
DHCP Server. The IP address for the Dynamic Host Configuration Protocol server that provides the TCP/IP configuration for all the computers that are connected to the router.

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

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

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

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

Mode. Indicates the wireless communication mode: Up to 54 Mbps, Up to 217 Mbps (default), and Up to 450 Mbps.

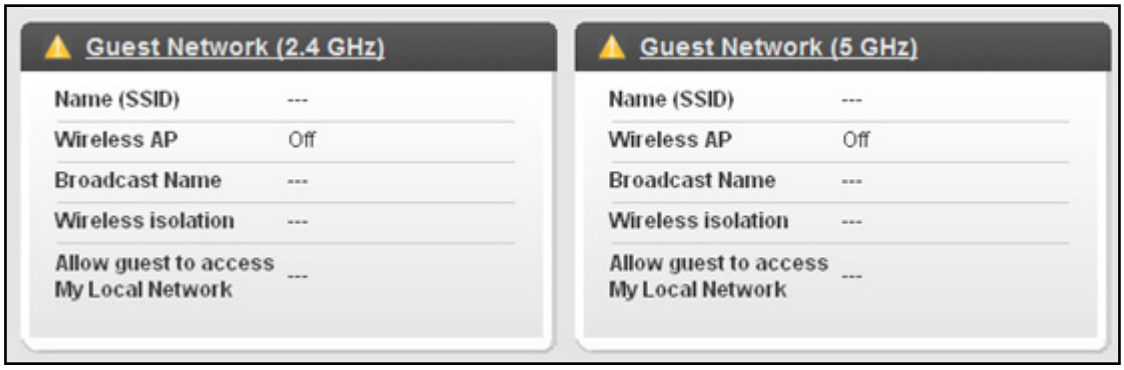
Wireless AP. Indicates whether the radio feature of the router is enabled. If this feature is not enabled, the Wireless LED on the front panel is off.

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 LED on the front panel is off.

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

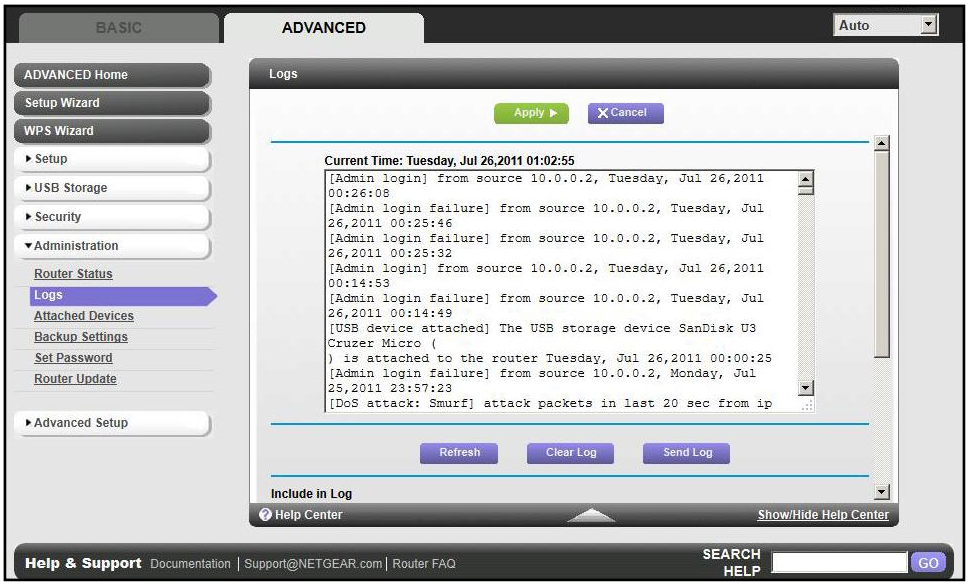
Wireless Isolation. Select this check box only if you want to prevent wireless connections to the router.

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

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

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.

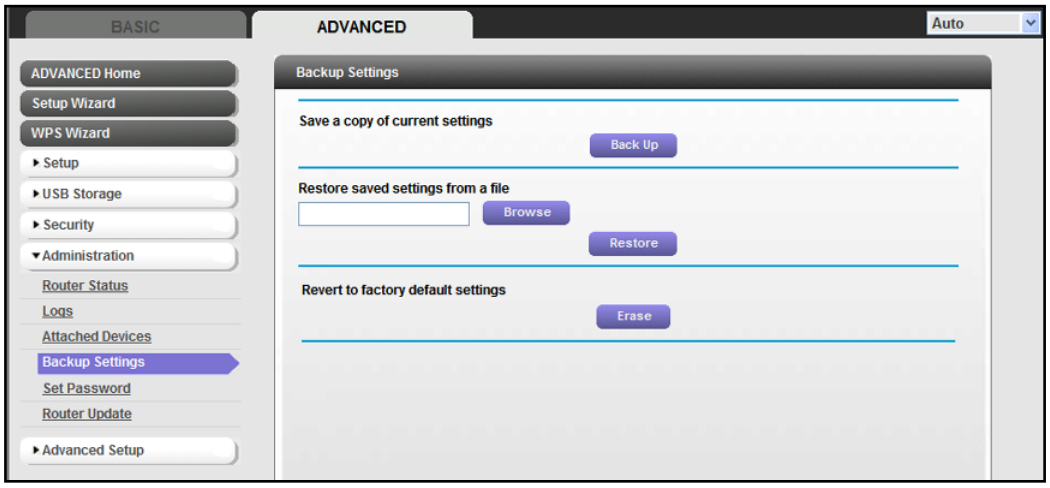
Manage the Configuration File

The configuration settings of the N900 Wireless Dual Band Gigabit Router are stored within the router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

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

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



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

Restore Configuration Settings

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

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

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 120), 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.

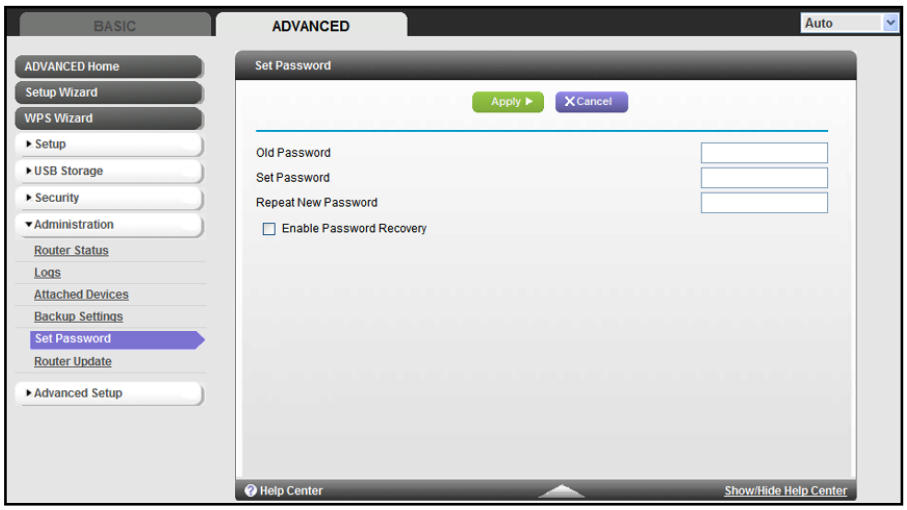
Set Password

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 11).

➢ **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 will 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.

Time Machine

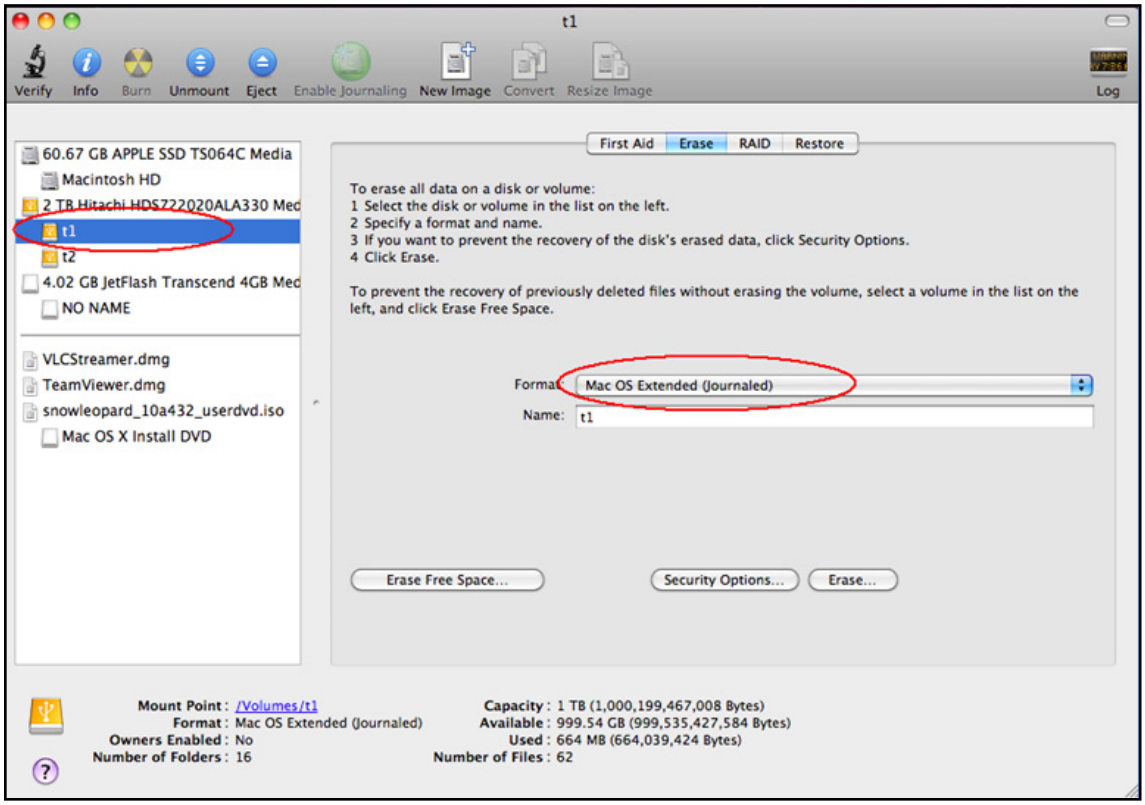
Time Machine works only on Mac computers. It automatically backs up everything on your computer to a USB hard drive that is connected to the Mac.

Set Up Time Machine

If you are already using Time Machine software with your USB hard drive, you can skip the set up and go directly to the following section, *Access the Connected USB Hard Drive*.

➢ **To set up Time Machine:**

1. Physically connect the USB hard drive to your Mac.
2. On your Mac, go to the magnifying glass at the top right of the desktop, and search for **disk utility**.
3. Open the Disk Utility and format your drive, as shown here.



The router supports GUID and MBR partitions only. To see how to change the partition scheme, see *Change the Partition Scheme* on page 85.

You can now use Time Machine wirelessly by connecting the USB hard drive to your C router.

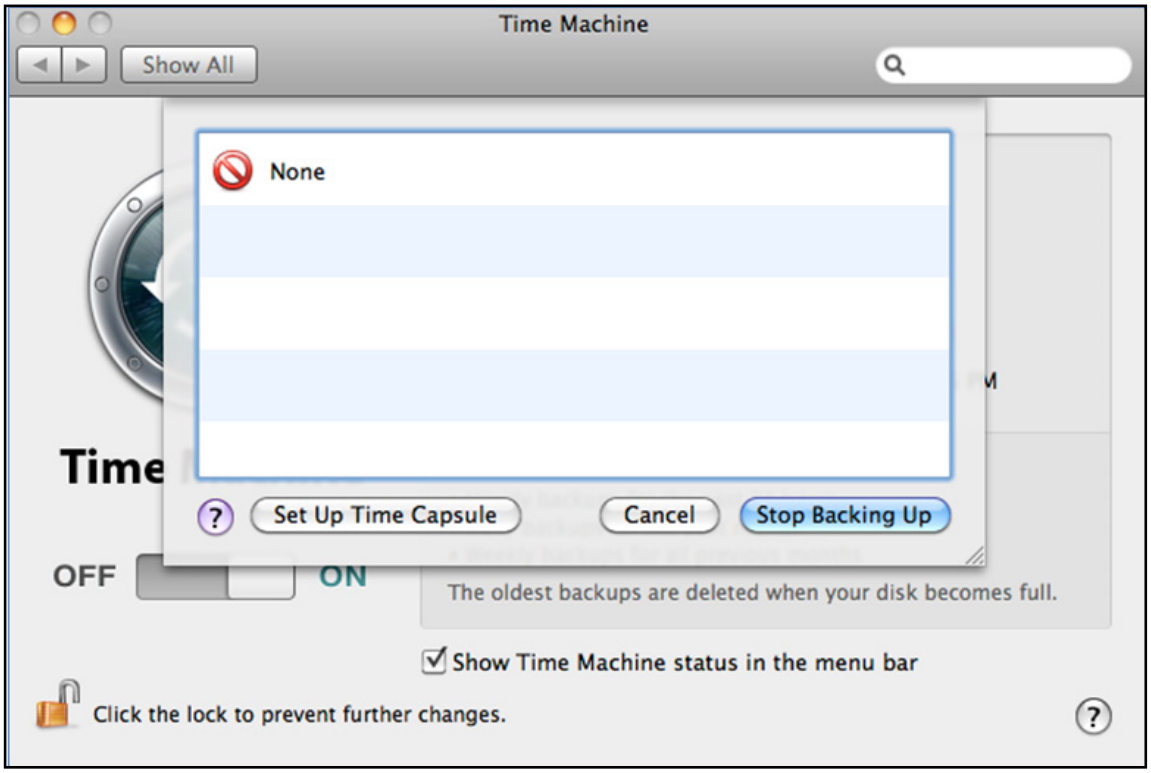
Access the Connected USB Hard Drive

After the initial set up explained in the previous section, you can access the connected USB hard drive from Your Mac or PC.

➢ **To access the drive:**

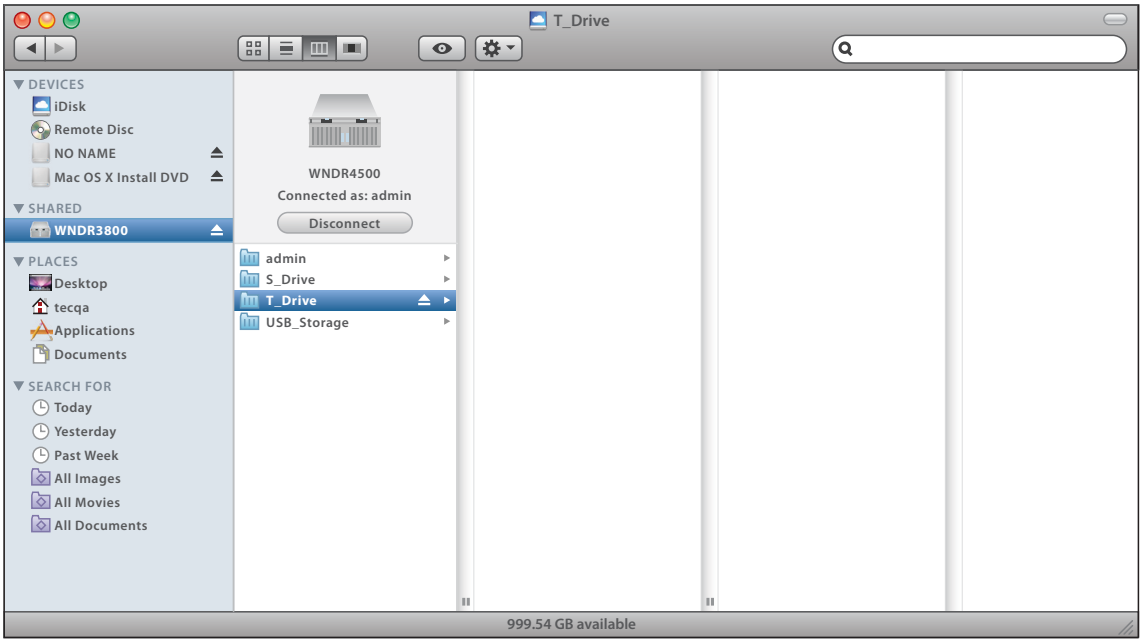
1. Start ReadySHARE:
   - On a Mac: Select **Go > Connect to Server,** and then type: **smb://readyshare**
   - On a PC: Select **Start > Run**, and then type: **\\readyshare**
2. From your MAC desktop, open **Macintosh HD**.
3. Click the **Connect As** button. In the pop-up window, select **Registered User**, and enter **admin** as the user name and **password** as the password. Click **Connect**.
   - After connecting successfully, you can list your connected devices. Note that you see one extra device, called *admin*, whenever you log in as **admin**.
   - If you are backing up a large amount of data, befor eyou contineu, see *Before You Back up a Large Amount of Data* on page 83.
4. From the Apple menu, select **System Preferences**. Open **Time Machine**. Click **Select Disk** and choose the backup disk. Click the **Use for Backup** button to complete your selection.

   If you do not see the USB partition that you want to use for backup in the Time Machine disk list, go to MAC finder, and click that USB partition.Then that device displays in the Time Machine list.



You are prompted to log in.

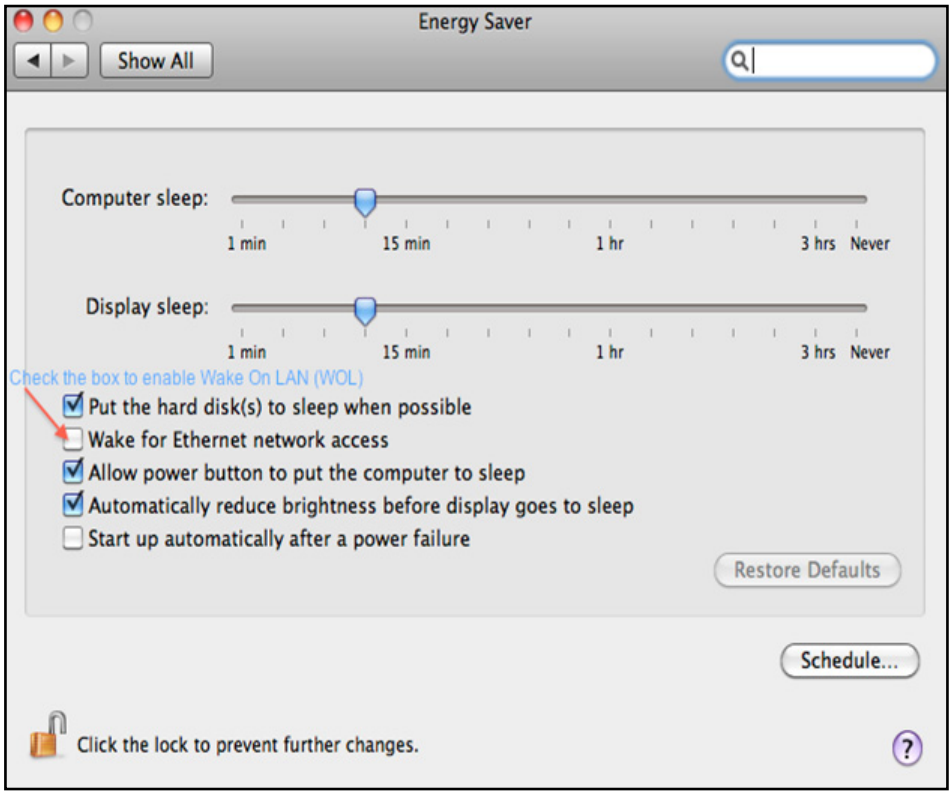
5. Enter the password (the same one you use to log in to the router as admin) and backup begins.



Before You Back up a Large Amount of Data

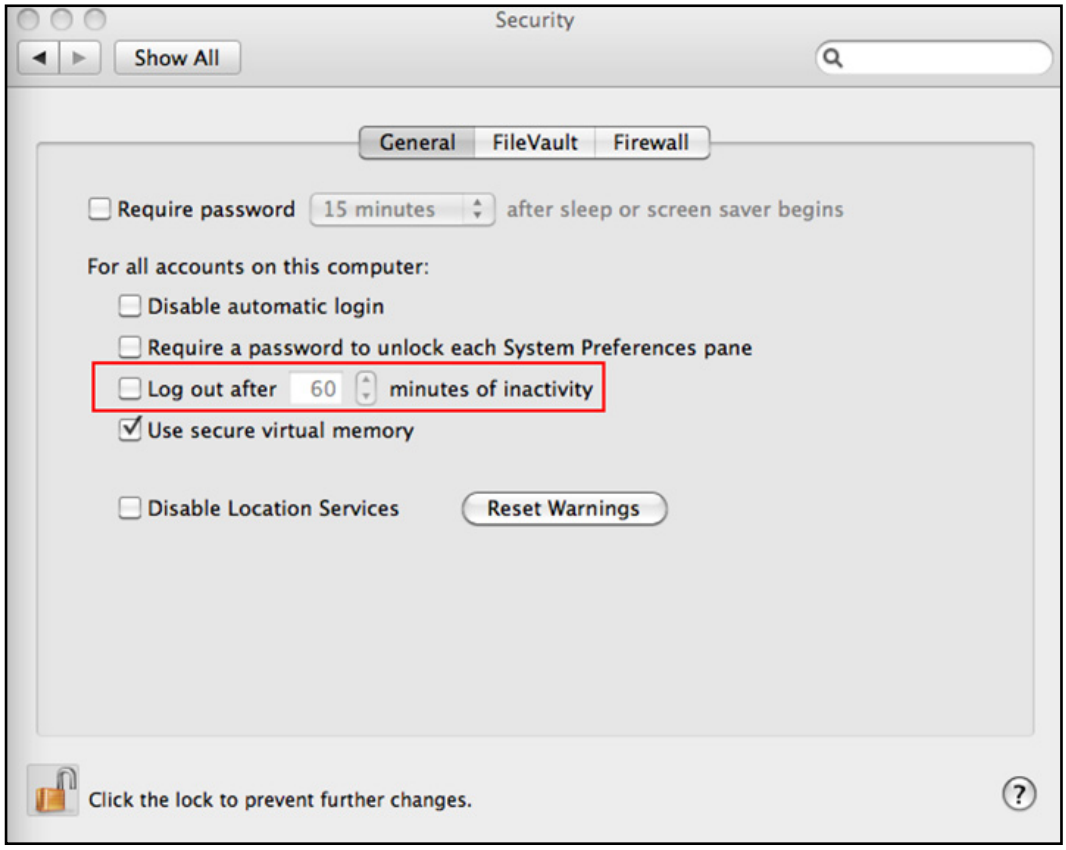
Before you back up a large amount of data with Time Machine, NETGEAR recommends that you do the following to ensure a successful operation:

1. Upgrade the operating system of the Mac machine.
2. Verify and repair the backup disk and the local disk.
3. Verify and repair the permissions on the local disk.
4. Set Energy Saver.
   a. From the Apple menu, select **System Preferences**.
   b. From the View menu, select **Energy Saver**.
   c. On the Energy Saver screen, select **Wake for Ethernet network access**.



   d. Click the Back arrow to exit this screen. Your changes will be saved.
5. Modify your Security settings.
   a. From the Apple menu, select **System Preferences**.
   b. From the View menu, select **Security**.

c. On the Security screen, leave the **Log out after minutes of inactivity** check box **cleared** (not selected).

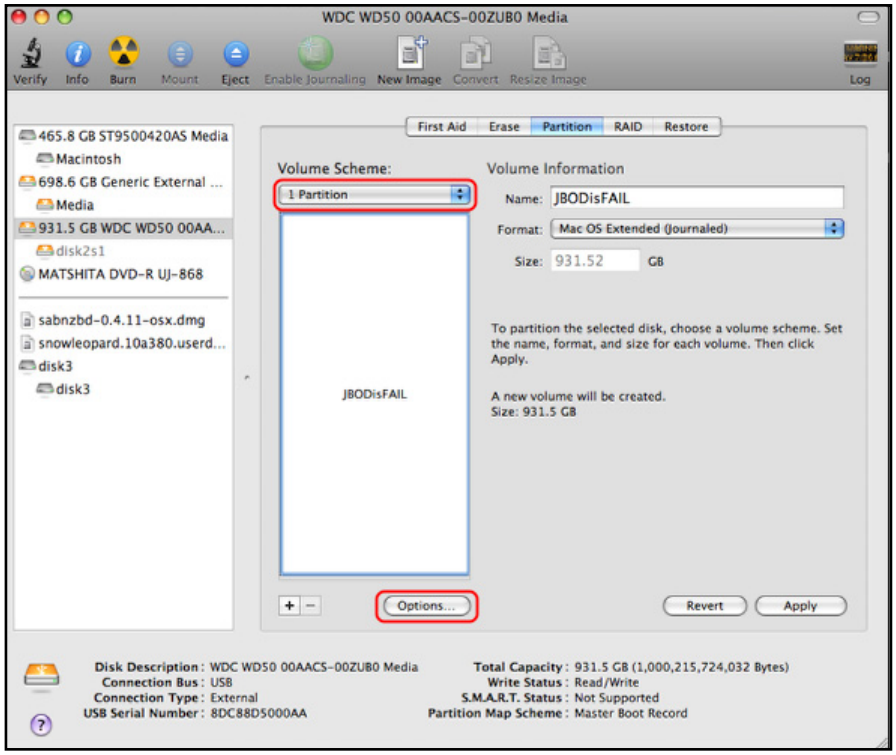


Change the Partition Scheme

To run with the router, the partition scheme on your Mac has to be set to either GUID or MBR.

➢ **To make sure the partition scheme is set to one of these supported schemes:**

1. Open the Disk Utility and select your USB drive.
2. Select the **Partition** tab.
3. Select **Volume Scheme** and set the number of partitions you would like to use.



4. Click **Options**, and the Partition options appear.
5. Select **GUID Partition Table** or **Master Boot Record** (MBR).
6. Click **OK**.

Advanced Settings

9

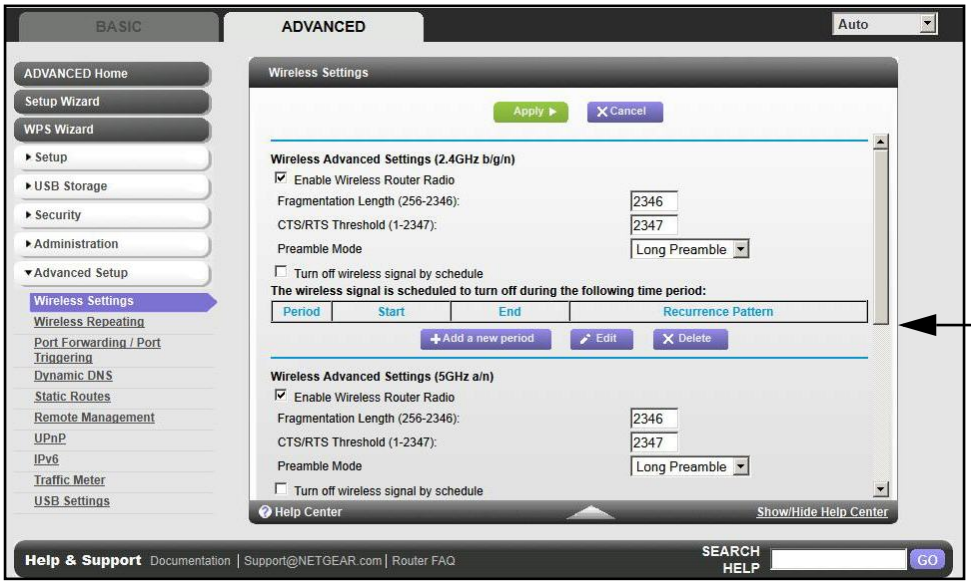
This chapter describes the advanced features of your router. The information is for users with a solid understanding of networking concepts who want to set the router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

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 instance, 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 WNDR4500v2 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 N900 Wireless Dual Band Gigabit Router up to be used as a wireless access point (AP). Doing 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.

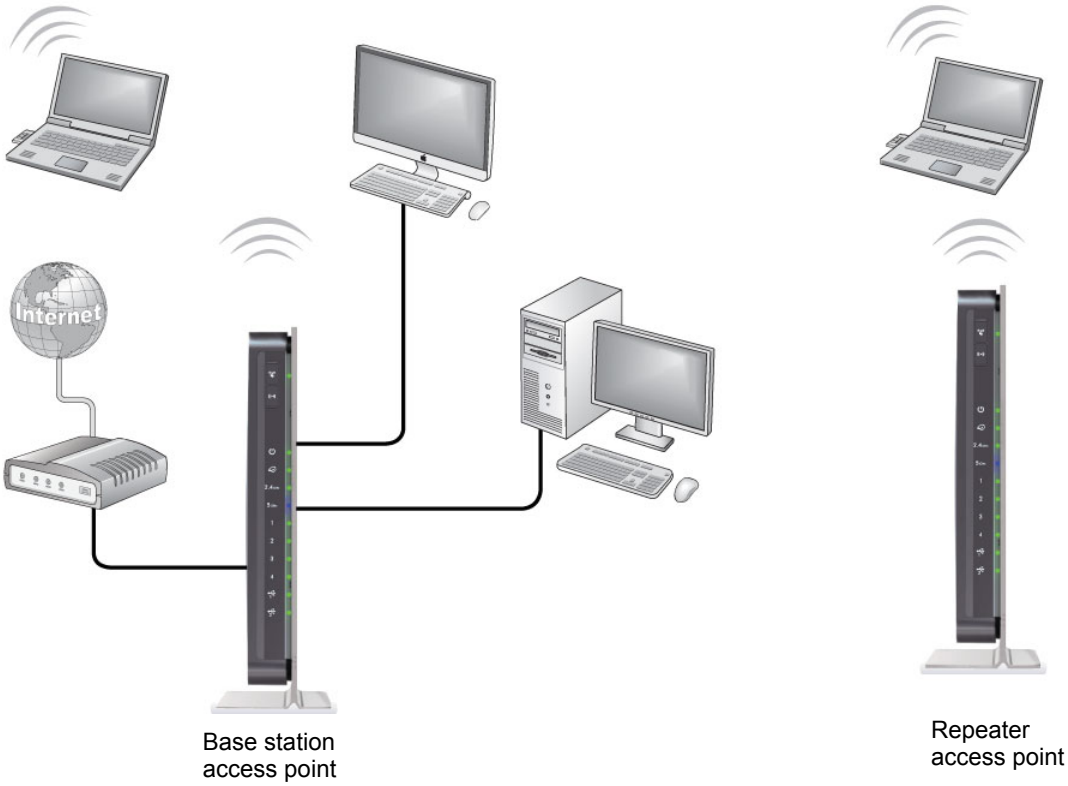


Figure 8. Wireless repeating scenario

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

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

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

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

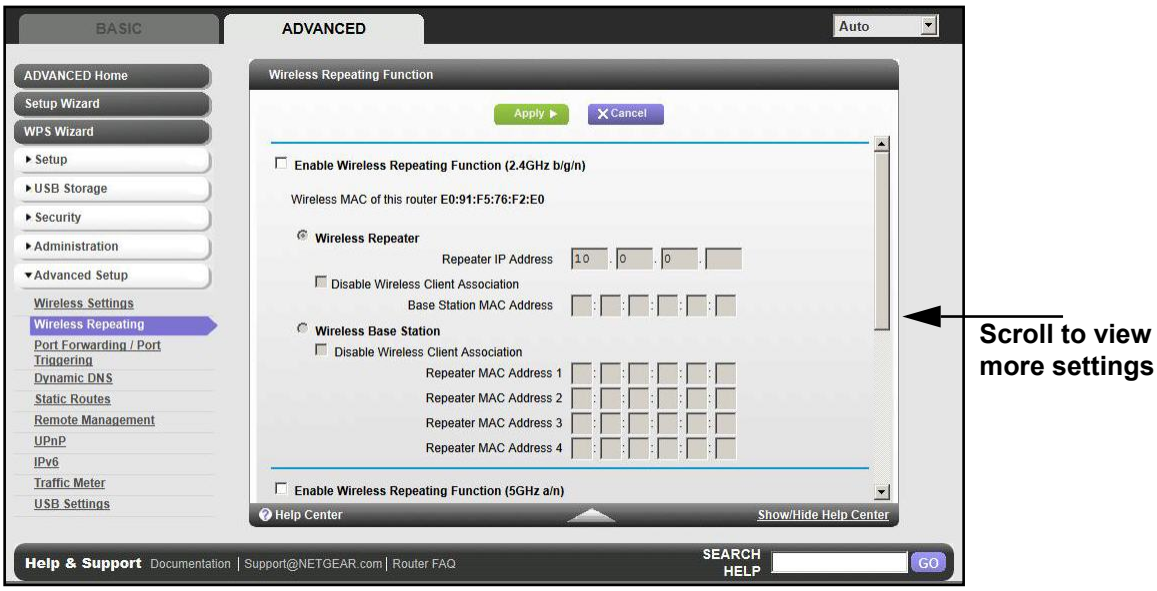
The WNDR4500v2 router is always in dual band concurrent mode, unless you turn off one radio. Be aware that if you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station 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 will 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 4 other access points. Enter the MAC addresses of the other access points in these fields.

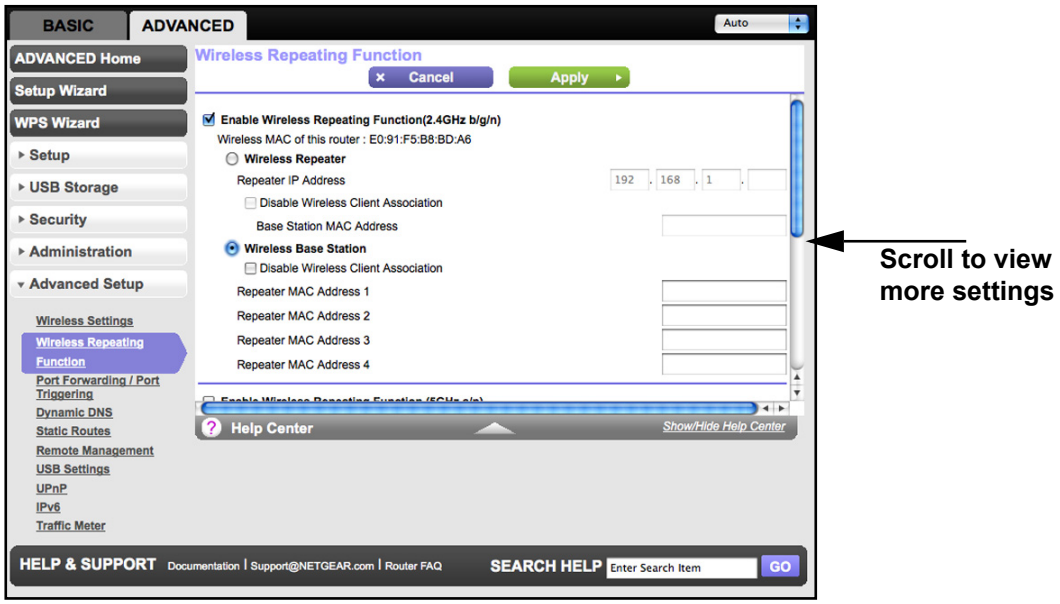
Set Up the Base Station

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

➢ **To set up the base station:**

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). Note that 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 WNDR4500v2 base station with a non-NETGEAR router as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

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

1. Log in to the router that will be the repeater. 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 address of the base station.

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

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

Port Forwarding and 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 is an active session 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 back 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 back 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 will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or 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 usually can determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

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

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.

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

Set Up Port Forwarding to Local Servers

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

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

Before starting, you need to determine which type of service, application, or game you want to provide, and the local IP address of the computer that will provide 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 N900 Wireless Dual Band Gigabit 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 97.
3. In the corresponding Server IP Address field, enter the last digit of the IP address of your local computer that will provide this service.
4. Click **Add**. The service appears in the list in the screen.

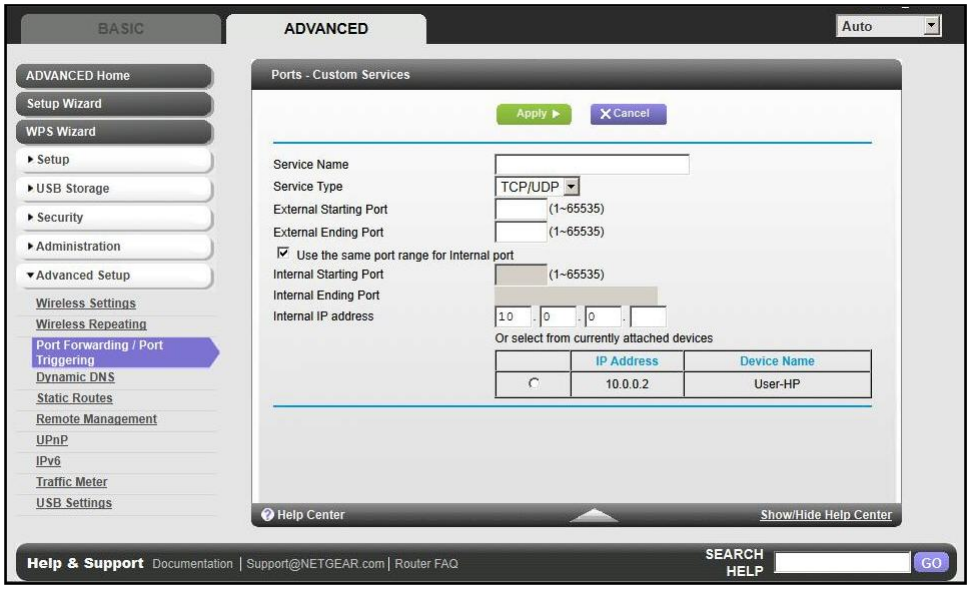
Add a Custom Service

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 will provide 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 will always give 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 101. To access your web server from the Internet, a remote user has to know the IP address that has been 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.

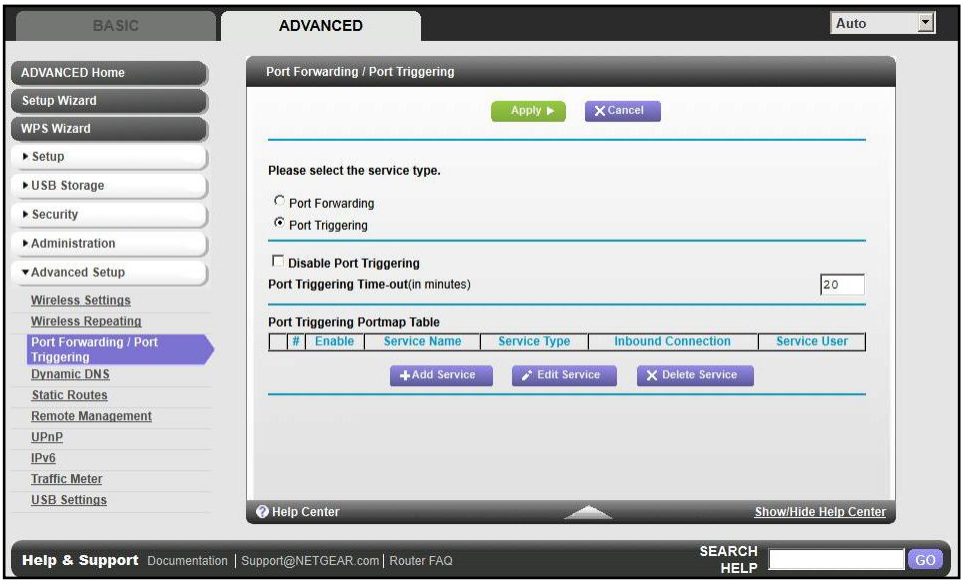
Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 106.

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 will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or 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.

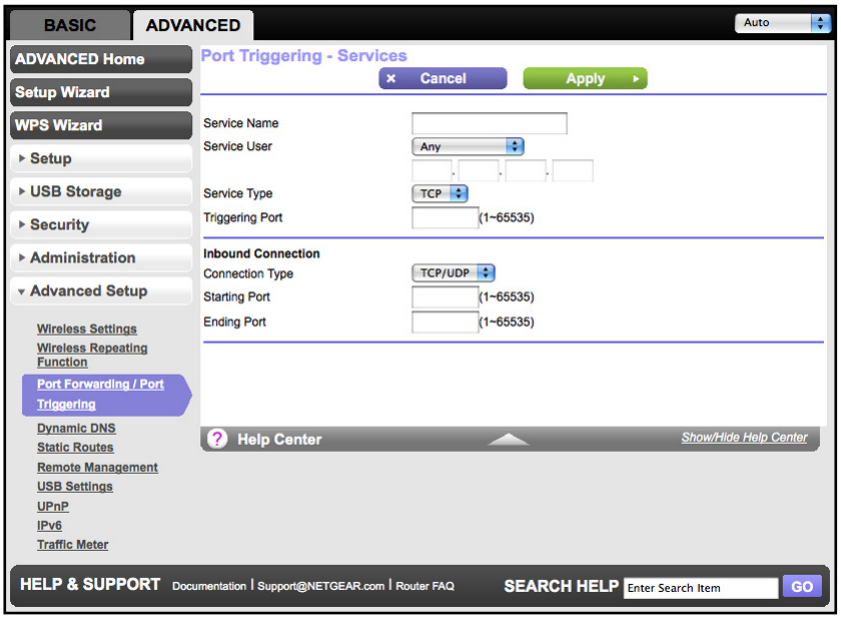


3. Clear the **Disable Port Triggering** check box if it is selected.

   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 will cause 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 will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service 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:

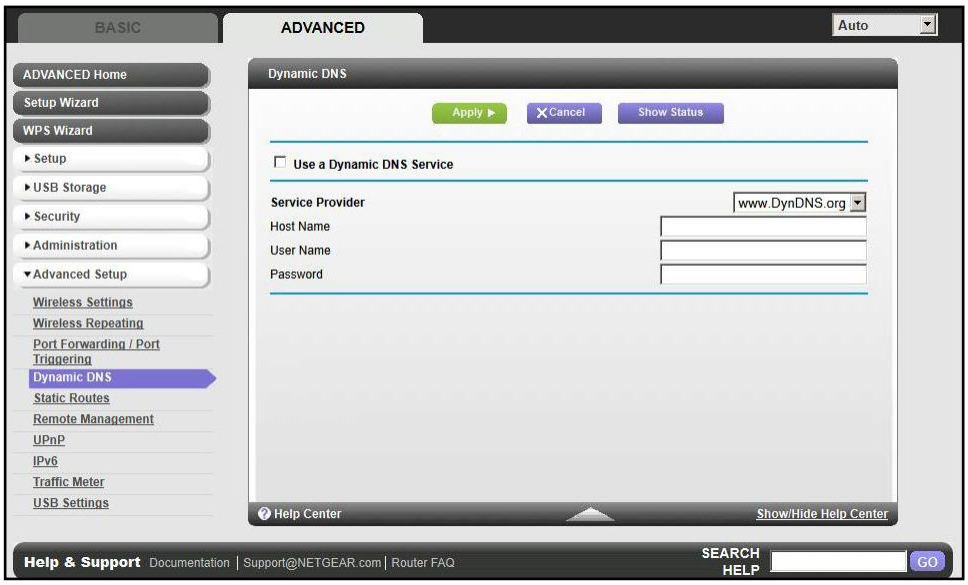


Figure 9. Forward traffic to a changing IP address

➢ **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.

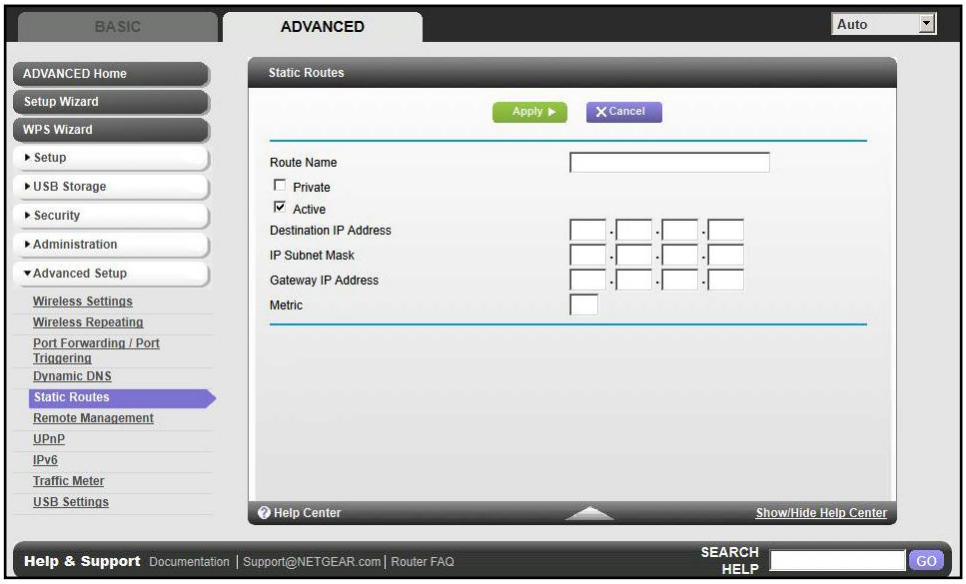
When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 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 will work 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 destination 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 N900 Wireless Dual Band Gigabit 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 N900 Wireless Dual Band Gigabit 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 very 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 to be allowed to access the router's remote management.

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

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.
- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address 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 nterface. 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 50 for the procedure.

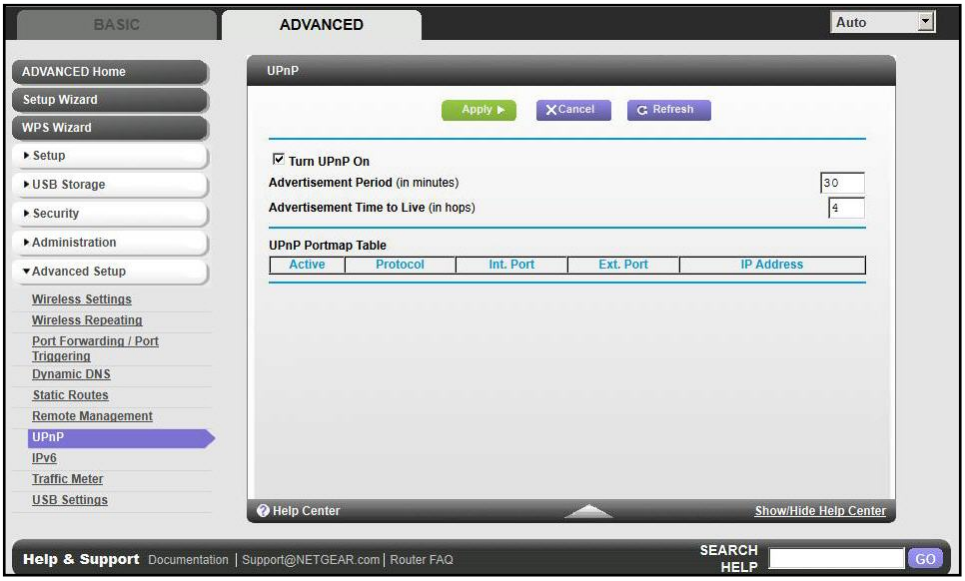
Universal Plug and Play

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, then 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.

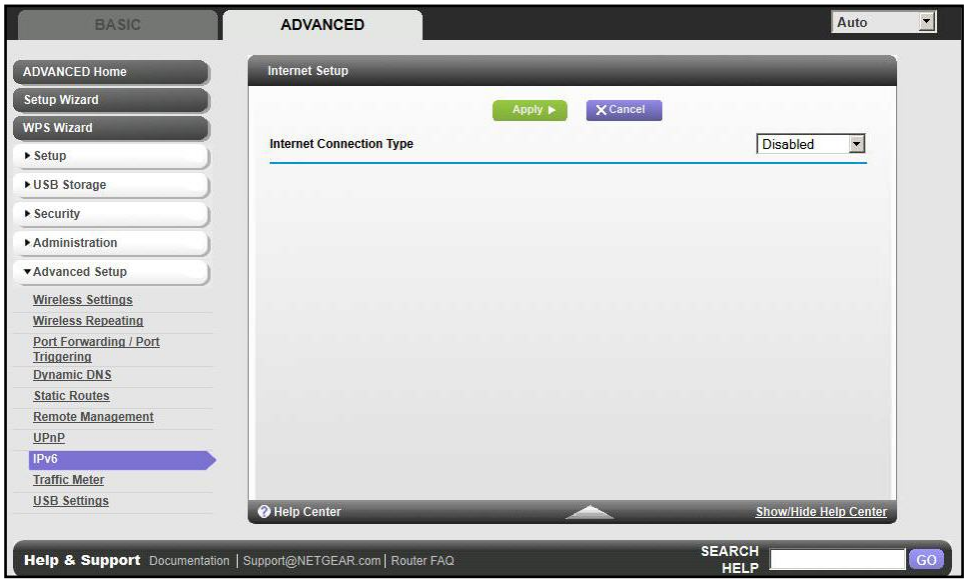
3. Click **Apply** to save your settings.

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:



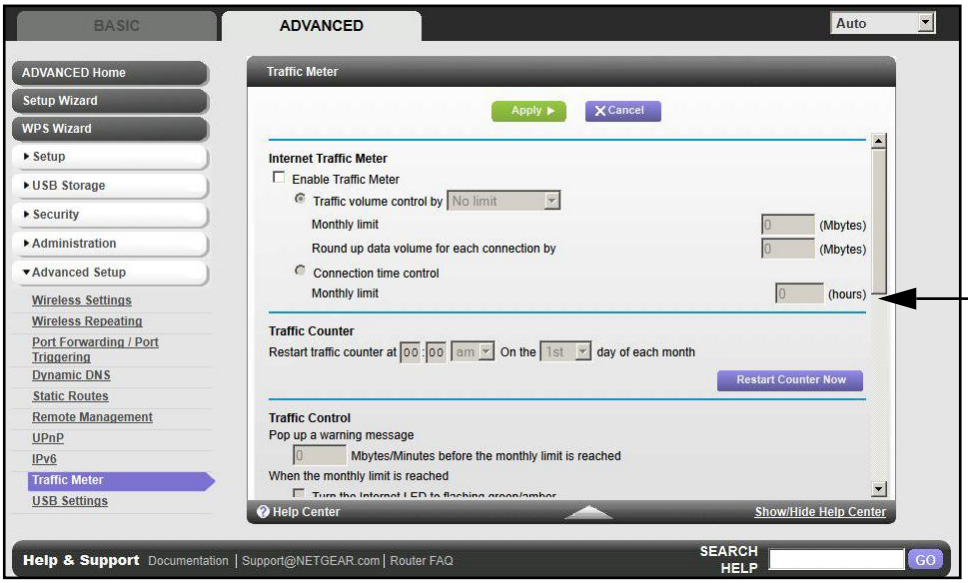
2. Select the IPv6 connection type from the list. Your Internet service provider (ISP) can provide this information.
   - If your ISP did not provide details, you can select **IPv6 Tunnel**.
   - If you are not sure, select **Auto Detect** so that the router detects the IPv6 type that is in use.
   -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



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.

10 Troubleshooting

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

This chapter contains the following sections:

- *Quick Tips*
- *Troubleshooting with the LEDs*
- *Cannot Log In to the Router*
- *Cannot Access the Internet*
- *Changes Not Saved*
- *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 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 on.
   - 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.
- Check that you are using the 12V DC, 2.5A power adapter that NETGEAR supplied for this product.
- If the Power/Test LED blinks slowly and continuously, the router firmware is corrupted. This can happen if a firmware upgrade is interrupted, or if the router detects a problem with the firmware. If the error persists, you have a hardware problem. For recovery instructions, or help with a hardware problem, contact technical support at *www.netgear.com/support.*

Power/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 you turn on power to the router:

1. Turn the power off and back on to see if the router recovers.
2. Press and hold the **Reset** button to return the router to its factory settings. as explained in *Restore the Factory Settings and Password* on page 117.

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 **Reset** button to return the router to its factory settings as explained in *Restore the Factory Settings and Password* on page 117.

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 could 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 has succeeded for the wireless device you are adding to the wireless network.
- Make sure you have not pressed the WPS button on the side 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 auto-generated 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 120.
- 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 *www.netgear.com*.
2. Access the router interface at **www.routerlogin.net.**
3. Select **Adminstration > 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 111.

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

- Your Internet service provider (ISP) might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Internet Setup screen.
- Your ISP allows only one Ethernet MAC address to connect to Internet and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.
  - Configure your router to clone your computer's MAC address.

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

- Your computer might not recognize any DNS server addresses.

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

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

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

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

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

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, then your PPPoE connection is up and 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 also might be a provisioning problem with your ISP.

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

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

Changes Not Saved

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

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

Wireless Connectivity

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

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

  If not, check the Wireless LEDs on the front of the router. It should be lit. If it is 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 **Wireless** see (*Basic Wireless Settings* on page 23).

  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 78).

- Use the Reset button on the back of the router. See *Factory Settings* on page 120. 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. Troubleshooting a network is made very easy by using the ping utility in your computer or workstation.

Test the LAN Path to Your Router

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

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

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 could 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 be 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 Setup screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers.

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

Supplemental Information

This appendix provides factory default settings and technical specifications for the N900 Wireless Dual Band Gigabit Router WNDR4500v2.

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 **Reset** button on the back of the router for at least 7 seconds. The router resets, and returns to the factory configuration settings shown in the following table.

Table 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 savings 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	WPA2-PSK (AES)
	Broadcast SSID	Enabled
	Transmission speed	Auto*
	Country/region	United States in the US; otherwise varies by region
	RF channel	6 until region selected
	Operating mode	Up to 450 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. WNDR4500v2 Router specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, 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 104º F)
Operating humidity	10% to 90% relative humidity, noncondensing
Electromagnetic Emissions	FCC Part 15 Class B EN 55 022 (CISPR 22), Class B C-Tick N10947
LAN	10BASE-T or 100BASE-Tx or 1000BASE-T, RJ-45
WAN	10BASE-T or 100BASE-Tx or 1000BASE-T, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for the previous table.
Radio data rates	Auto Rate Sensing
Data encoding standards	IEEE 802.11n 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. WNDR4500v2 Router specifications (continued)

Feature	Description
Operating frequency range	2.4 GHz 2.412–2.462 GHz (US) 2.412–2.472 GHz (Europe ETSI) 5 GHz 5.18–5.24 + 5.745–5.825 GHz (US) 5.18–5.24 GHz (Europe ETSI)
802.11 security	WEP, WPA-PSK, WPA2-PSK, and WPA/WPA2

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.

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

Europe - EU Declaration of Conformity

CE !

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328 (2.4Ghz), EN301 489-17, EN301 893 (5Ghz), EN60950-1

For complete DoC, visit the NETGEAR EU Declarations of Conformity website at:
http://support.netgear.com/app/answers/detail/a_id/11621/

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

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 N900 Wireless Dual Band Gigabit Router WNDR4500v2 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.

This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N900 Wireless Dual Band Gigabit Router WNDR4500v2) 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.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible

Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

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.

IMPORTANT NOTE: Radiation Exposure Statement:

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

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

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

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.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

Le dispositif pourrait automatiquement cesser d'émettre en cas d'absence d'informations à transmettre, ou une défaillance opérationnelle. Notez que ce n'est pas l'intention d'interdire la transmission des informations de contrôle ou de signalisation ou l'utilisation de codes répétitifs lorsque requis par la technologie.

GPL License Agreement

GPL may be included in this product; to view the GPL license agreement go to *ftp://downloads.netgear.com/files/GPLnotice.pdf.*

For GNU General Public License (GPL) related information, please visit *http://support.netgear.com/app/answers/detail/a_id/2649* .

Interference Reduction Table

The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

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

Index

A

access
  remote 105
  viewing logs 75
access points 88
accessing remote computer 92
adding
  custom service 97
  priority rules 39
address reservation 37
advertisement period 107
alerts, emailing 68
applications, QoS for online gaming 39
approved USB devices 50
attached devices 21
authentication, required by mail server 68
automatic firmware checking 70
automatic Internet connection 29

B

back panel 11
backing up configuration 77
base station, setting up 90
blocking
  inbound traffic 92
  keywords 64
  services 65
  sites 64
box contents 8

C

cables, checking 111
changes not saved, router 117
compliance 124
configuration file 77
configuring
  DMZ server 33
  Dynamic DNS 102
  NAT 32
  port forwarding 96
  port triggering 99
  QoS 38
  repeater unit 91
  user-defined services 65
connecting wirelessly 8
country setting 29
crossover cable 113
CTS/RTS Threshold 87
custom service (port forwarding) 97

D

dashboard 16
data packets, fragmented 33
default DMZ server 33
default factory settings, list of 120
default factory settings, restoring 78, 117
default gateway 73
deleting
  configuration 78
  keywords 64
denial of service (DoS) protection 63
devices, attached 21
DHCP server 36, 73
DHCP setting 72
DMZ server 33
DNS addresses
  troubleshooting 115
DNS servers 92
Domain Name Server (DNS) addresses 20, 72
Dynamic DNS 101
DynDNS.org 101

E

electromagnetic emissions 122
email notices 68
encryption keys 27
erasing configuration 78
Ethernet cables, checking 111
Ethernet LED, troubleshooting and 112, 113

F

factory default settings, restoring 78, 117
factory settings
  list of 120
  resetting 11
file sharing 44
firmware version 71
firmware, upgrading 15, 70
fragmentation length 87
fragmented data packets 33
front panel 9

G

games, online, QoS for 39
gateway IP address 20
genie, NETGEAR 14
guest networks 26, 75

H

host name 19
host, trusted 64

I

inbound traffic, allowing or blocking 92
installing NETGEAR genie 14
installing with the Setup Wizard 29
Internet connection
  setting up 19
  troubleshooting 114
Internet LED, troubleshooting and 112
Internet port 29, 71
Internet Relay Chat (IRC) 94
Internet service provider (ISP)
  account information 13
  Internet Setup screen 19
  login 13
Internet services, blocking access 65
Internet Setup screen 19
interval, poll 72
IP addresses
  current 71
  DHCP 13
  dynamic 101
  reserved 37
IP subnet mask 72

K

keywords 64

L

label, product 11
LAN port
  QoS for 40
  settings 71
LAN setup 35
language setting 29
large files, sharing 45
lease, DHCP 73
LEDs
  described 10
  troubleshooting and 112
local servers, port forwarding to 96
logging in 13, 15
logs
  emailing 68
  viewing 75

M

MAC addresses
  current 71
  product label 11
  QoS for 41
mail server, outgoing 68
maintenance settings 69
managing router remotely 105
media server, setting the router to be a 50
menus, described 16
metric value 104
mixed mode security options 27
MTU size 33
multicasting 36

N

NAT (Network Address Translation) 32, 33, 93
NETGEAR genie 14
network, how to restart 111
networks
  guest 75
networks, guest 26
networks, troubleshooting 111

O

outgoing mail server 68

P

packets, fragmented 33
Parental Controls 22
passphrases
  changing 25
  product label 11
password recovery, admin 79
password, restoring 117
photos, sharing 45
poll interval 72
port filtering 65
port forwarding 92, 94, 95, 96
port numbers 65
port status 72
port triggering 92, 93, 95, 99
ports,listed, back panel 11
positioning the router 8
Power LED, troubleshooting and 112
PPPoE (PPP over Ethernet) 115
Preamble mode 87
preset security
  about 23
  passphrase 25
pre-shared key 27
primary DNS addresses 20
printing files and photos 45
prioritizing traffic 38
Push 'N' Connect 17

Q

QoS (Quality of Service) 38

R

radio, wireless 87
range of wireless connections 8
ReadySHARE access 44, 47
recovering admin password 79
releasing connection status 73
remote management 105
renewing connection status 73
repeater units 91
reserved IP adresses 37
reset button 120
restarting network 111
restoring
  configuration file 77
  default factory settings 78, 117
router interface, described 16
router status, viewing 71

S

scheduling keyword and service blocking 67
secondary DNS 20
security 23
  firewall settings 63
  see also security options
security options 27
security PIN 11, 30
sending logs by email 68
serial number, product label 11
services, blocking 65
settings, default. *See* default factory settings
Setup Wizard 29
sharing files 44
sites, blocking 64
SMTP server 68
specifications,technical 120
SSID, described 25
static routes 103
status, router, viewing 71
subnet mask 72
system up time 72

T

technical specifications 120
technical support 2
Temporal Key Integrity Protocol (TKIP) 27
time to live, advertisement 107
time-out, port triggering 100
trademarks 2
traffic metering 109
troubleshooting 110
  log in access 114
  router changes not saved 117
trusted host 64

U

Universal Plug and Play (UPnP) 106
up time, system 72
upgrading firmware 15, 70
USB
  advanced configuration 48
  basic storage settings 46
  drive requirements 44
  file sharing 44

ReadySHARE access 44, 47
remote computer connection 52
specifying approved devices 50
unmounting a USB drive 49
USB devices, approved 50
user-defined services 65

V

viewing
logs 75
router status 71

W

WAN IP address, troubleshooting 114
WAN setup 32
Wi-Fi Protected Setup (WPS) 17, 30
devices, adding 17
wireless channel 25
wireless connection, troubleshooting 117
wireless connections 8
wireless devices,adding to the network 17
Wireless Distribution System (WDS) 88, 89
Wireless LED, troubleshooting and 113, 114
wireless mode 25
wireless network name (SSID)
broadcast 25
described 25
product label 11
wireless network settings 25
wireless radio 87
wireless repeating 88, 89
base station 90
repeater unit 91
wireless security options 27
wireless settings 23, 75
checking for correct 111
SSID broadcast 25
WMM (Wi-Fi Multimedia) 38
WPA encryption 27
WPA2 encryption 27
WPA2-PSK encryption 27
WPA-PSK/WPA2-PSK mixed mode 27
WPS button 17
WPS-PSK encryption 27
WPS-PSK+ WPA2-PSK encryption 27