NETGEAR

N150 Wireless ADSL2+ Modem Router DGN1000

User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

February 2012
202-10927-01
v1.0

into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at:
http://support.netgear.com.

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

Phone (Other Countries): Check the list of phone numbers at:
http://support.netgear.com/app/answers/detail/a_id/984.

Trademarks

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Contents

Chapter 4 Security Settings

Chapter 5 Network Maintenance

Chapter 6 Advanced Settings

Hardware Setup

1

Get to know your wireless modem router

The N150 Wireless ADSL2+ Modem Router DGN1000 provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). The N150 Modem Router has a built-in DSL modem and is compatible with all major DSL Internet service providers. The security features let you block unsafe Internet content and applications, and protect the devices that you connect to your home network.

If you have not already set up your new router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Router Internet Setup* on page 17, explains how to set up your Internet connection.

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

This chapter contains the following sections:

Unpack Your New Router

Your box should contain the following items:

- N150 Wireless ADSL2+ Modem Router DGN1000
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Microfilters and splitters (quantity and type vary by region)
- *Resource CD* with NETGEAR Genie setup
- Installation guide that explains how to cable and set up your router

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair. See *Position Your Wireless Router* on page 12 for information about where to place and how to position your router.

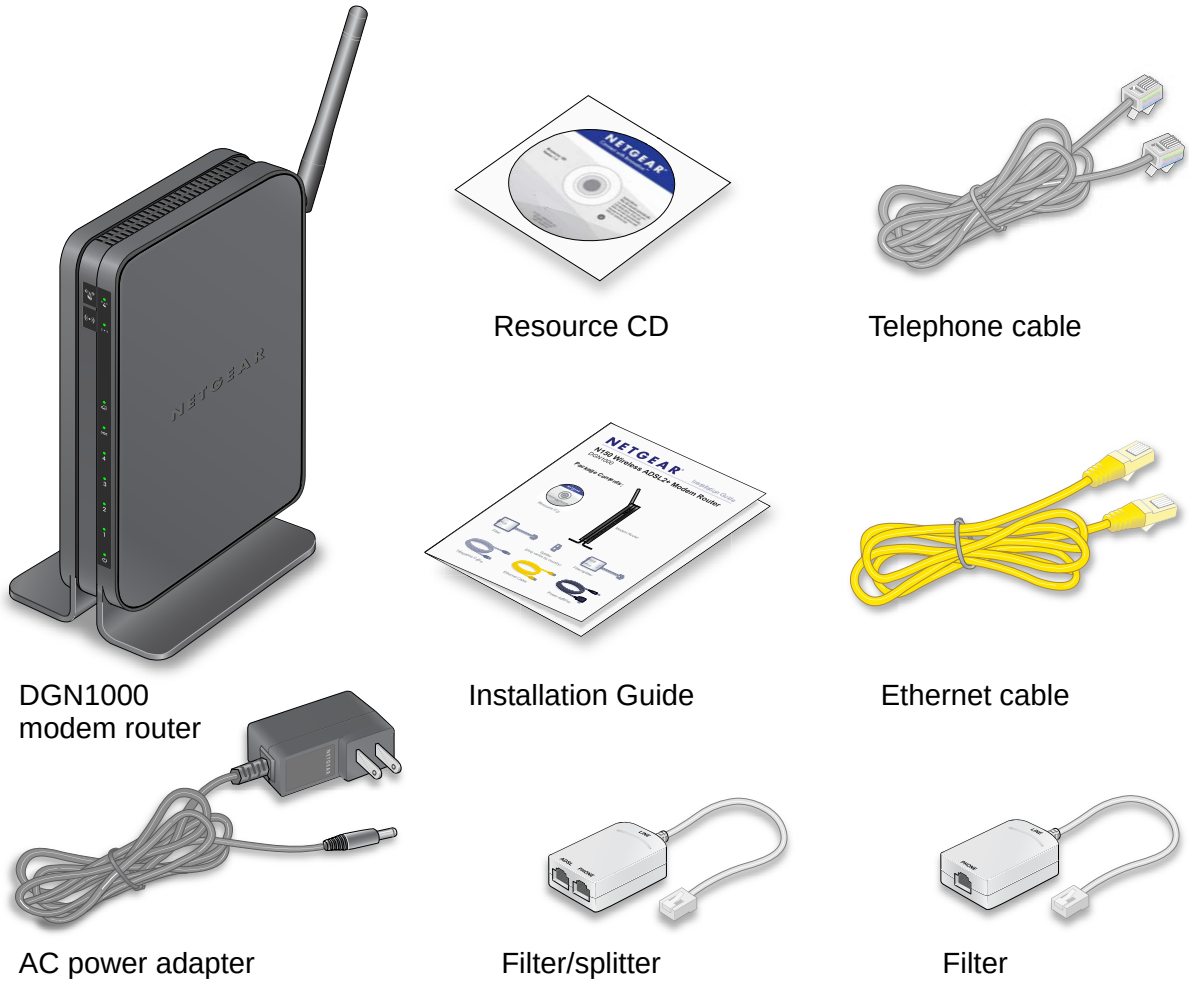


Figure 1. Review the box contents

Hardware Features

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

Label

The label on the bottom of the wireless modem router shows the router's Restore Factory Settings button, preset wireless information, MAC address, and serial number.

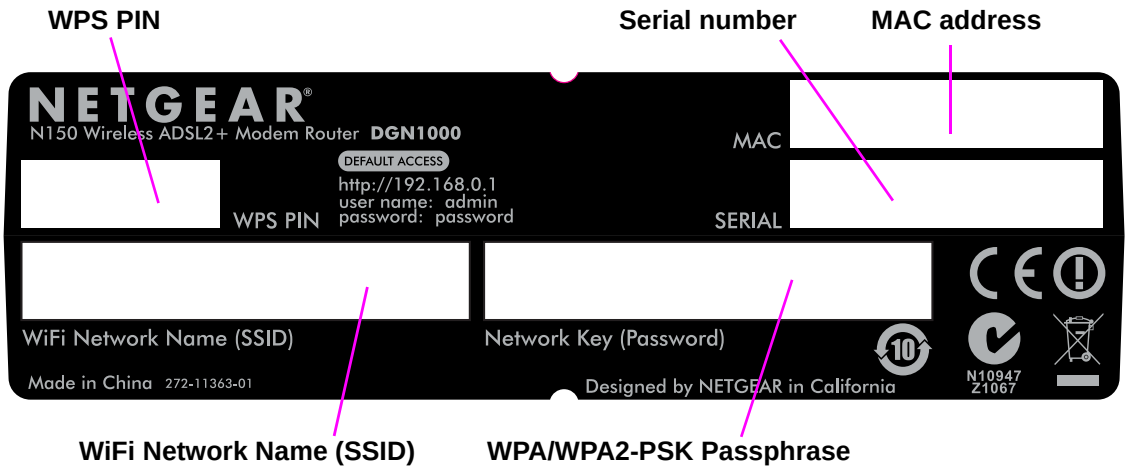


Figure 2. Information on the router label

See *Preset Security* on page 32 for information about preset security and MAC addresses. See *Factory Settings* on page 94 for information about the Restore Factory Settings button and the factory setting values.

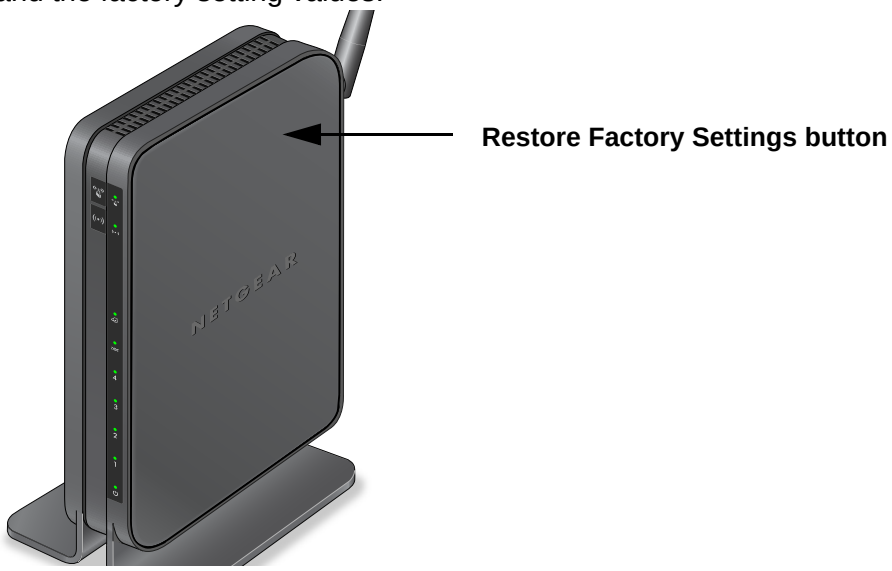


Figure 3. Location of Restore Factory Settings button

Back Panel

The back panel has the On/Off button and the port connections shown in the following figure:

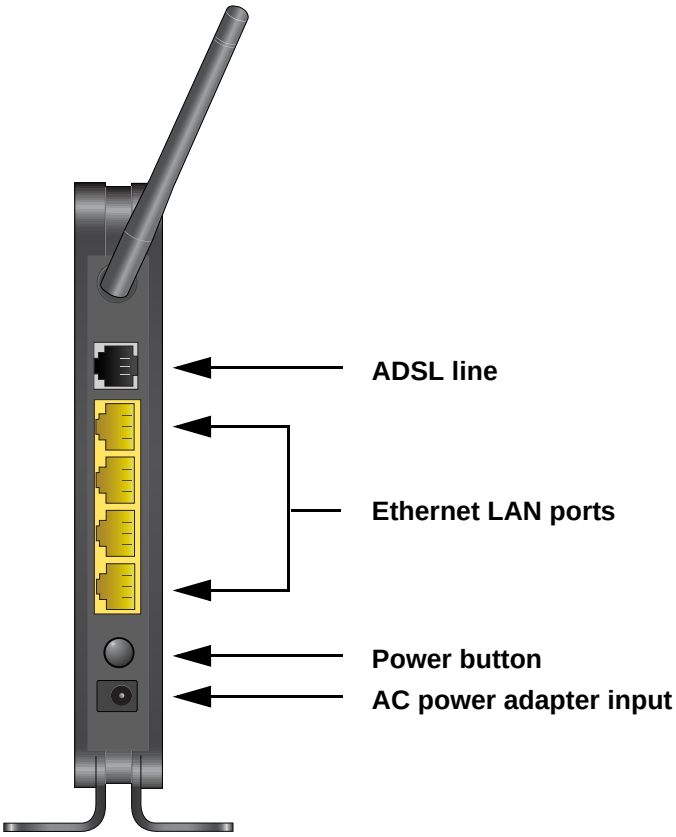


Figure 4. Back panel port connections

Viewed from left to right, the rear panel contains the following elements:

1. RJ-11 Asynchronous DSL (ADSL) port for connecting the wireless modem router to a DSL line

> ***Note:*** An ADSL port is capable of sending data over a DSL line at one speed and receiving it at another speed.

2. Four Ethernet RJ-45 LAN ports to cable the wireless modem router to the local computers
3. Power button to turn the router on and off.
4. AC power adapter input

Front Panel

The following figure shows the status LEDs and icons on the wireless modem router front panel. Note that the Wireless and WPS icons are buttons.

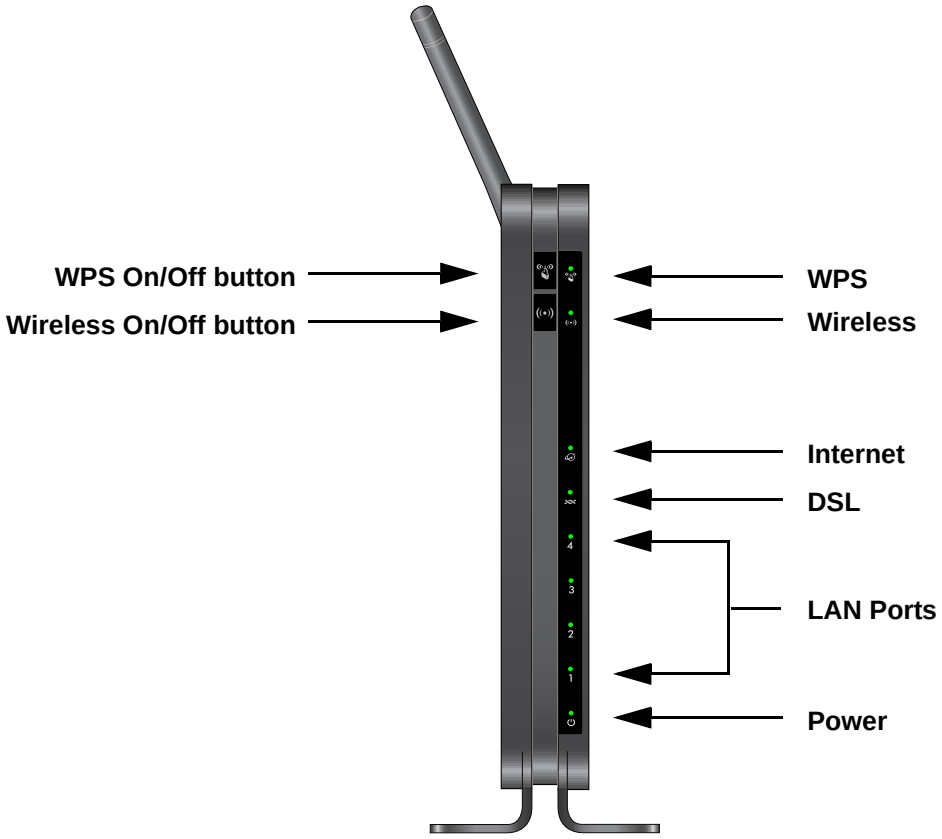


Figure 5. Front panel LED Icons

The tables describe the LEDs, icons, and buttons on the front panel from left to right.

Table 1. Power On/Off button

Icons	LED Activity	Description
	Solid green.	Power is supplied to the router.
	Solid red	POST (power-on self-test) failure or a device malfunction has occurred.
	Off	Power is not supplied to the router.
	Restore Factory Settings	Light blinks momentarily when the Restore Factory Settings button on the bottom of the unit is pressed for 6 seconds. The Power LED then blinks red three times when the Restore Factory Settings button is released and then turns green as the gateway resets to the factory defaults.

Table 2. LAN LED

icon	LED Activity	Description
	Solid green.	The LAN port has detected an Ethernet link with a device.
	Blinking Green	Data is being transmitted or received.
	Off	No link is detected on this port.

Table 3. DSL LED

Icon	LED Activity	Description
	Solid green.	You have a DSL connection. In technical terms, the DSL port is synchronized with a network-access device of an ISP.
	Blinking green	Indicates that the wireless modem router is negotiating the best possible speed on the DSL line.
	Off	The unit is off or there is no IP connection.

Table 4. Internet LED

Icon	LED Activity	Description
	Solid green	You have an Internet connection. If this connection is dropped due to an idle time-out but the DSL connection is still present, the light stays green. If the Internet connection is dropped for any other reason, the light turns off.
	Solid red	The Internet (IP) connection failed. See *No Internet Connection* on page 87 for troubleshooting information.
	Blinking green	Data is being transmitted over the DSL port.
	Off	No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection).

Table 5. Wireless Button and LED

Icon	LED Activity	Description
 Icon is on the Wireless button	Solid green.	There is wireless connectivity.
	Blinking green	Data is being transmitted or received over the wireless link.
	Off	There is no wireless connectivity. Plug an Ethernet cable into one of the LAN ports to get wired connectivity. See *Turn Off Wireless Connectivity* on page 33 for more information about the use of this button.

Table 6. WPS Button and LED

Icon	LED Activity	Description
 Icon is on the WPS button	Solid green.	Indicates that wireless security is enabled.
	Blinking green	A WPS-capable device is connecting to the device.
	Off	WPS is not enabled. See *Wi-Fi Protected Setup (WPS) Method* on page 35 for more information about the use of this button.

Position Your Wireless Router

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

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the wireless modem router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference. These sources include ceiling fans, home security systems, microwaves, PCs, or the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.
- With the antenna in a vertical position to provide the best side-to-side coverage or with the antenna in a horizontal position to provide the best up-and-down coverage, as applicable.

Also be aware that when you use multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels. For example, use Channels 1 and 6, or 6 and 11.

ADSL Microfilters

If this is the first time you have cabled a wireless router between a DSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your N150 Wireless Modem Router* on page 14.

An ADSL microfilter is a small in-line device that filters DSL interference out of standard phone equipment that shares the same line with your DSL service. Every telephone device that connects to a telephone line that provides DSL service, needs an ADSL microfilter to filter out the DSL interference. Example devices are telephones, fax machines, answering machines, and caller ID displays. Note that not every phone line in your home necessarily carries DSL service. The need for DSL service depends on the DSL service setup in your home.

Note: Often the ADSL microfilter is included in the box with the wireless modem router. If you purchased the wireless modem router in a country where a microfilter is not included, you have to acquire the ADSL microfilter separately.

One-Line ADSL Microfilter

➢ **To use a one-line ADSL microfilter:**

1. Plug the ADSL microfilter into the DSL line outlet on the wall.
2. Plug your phone equipment into the jack labeled Phone.

   The wireless modem router plugs directly into a separate DSL line. If you plug the wireless modem router into the phone jack, it blocks the Internet connection.

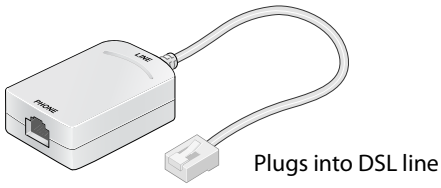


Figure 6. One-line ADSL microfilter

If you do not have a separate DSL line for the router, the best thing to do is to use an ADSL microfilter with a built-in splitter. See *Two-Line ADSL Microfilter* on page 14. You can also purchase a separate splitter.

➢ **To use a separate splitter:**

1. Insert the splitter into the phone outlet.
2. Connect the one-line filter to the splitter.
3. Connect the phone to the filter.

4. Plug the router into one of the other outlets in the separate splitter.

Two-Line ADSL Microfilter

Use an ADSL microfilter with a built-in splitter when there is a single wall outlet that provides connectivity for both the wireless modem router and your telephone equipment.

➢ **To use a two-line ADSL microfilter:**

1. Plug the ADSL microfilter into the DSL outlet on the wall.
2. Plug your phone equipment into the jack labeled Phone.
3. Plug the wireless modem router into the jack labeled ADSL.

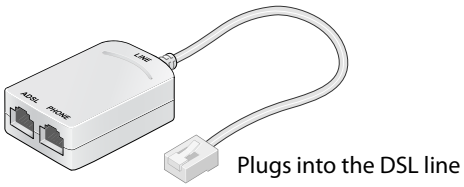


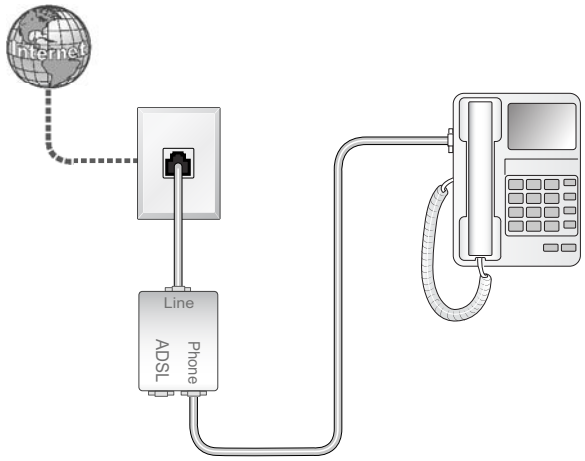
Figure 7. Two-line ADSL microfilter with built-in splitter

Cable Your N150 Wireless Modem Router

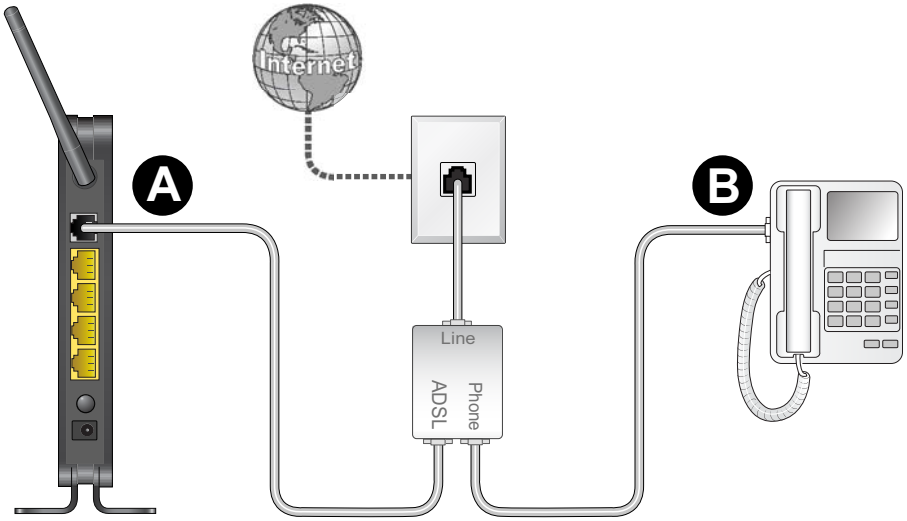
The installation guide that came in the box has a cabling diagram. This section walks you through how to cable your router with detailed illustrations.

➢ **To cable your router:**

1. Put an ADSL microfilter between the phone line and the phone as shown here. The illustration shows a two-line ADSL microfilter with a built-in splitter. The phone plugs into the Phone jack as shown.



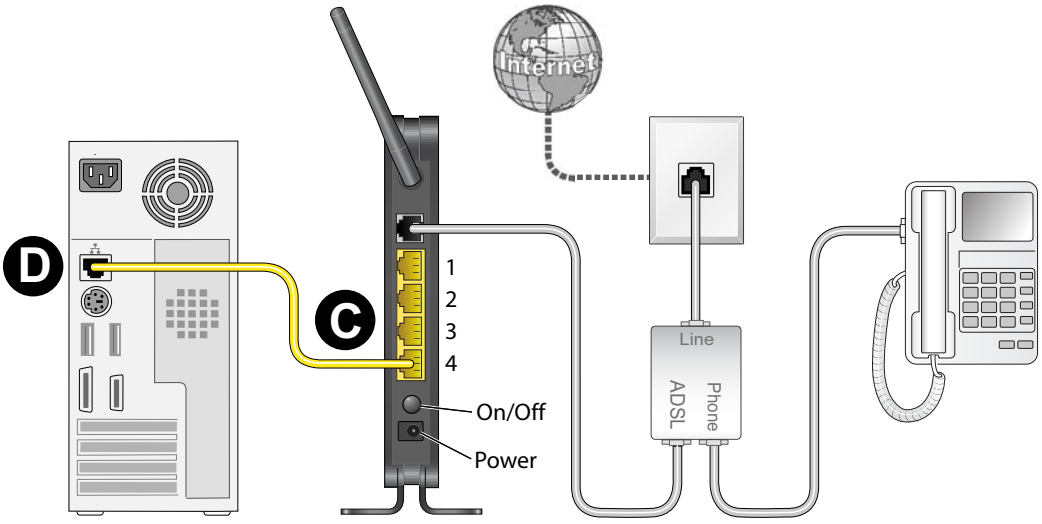
2. Use the included phone cable with RJ-11 jacks to connect the ADSL port (A) of the wireless modem router to the ADSL port (B) of the two-line ADSL microfilter.



CAUTION:

Incorrectly connecting a filter to your wireless modem router blocks your DSL connection.

3. Connect the Ethernet cable (C) from a wireless modem router LAN port to the Ethernet adapter (D) in your computer..



4. Plug the power adapter into the AC power adapter input (labeled Power), and plug the other end into a power outlet.

5. Connect any additional wired PCs to your router by inserting an Ethernet cable from a PC into one of the three remaining LAN ports.

Verify the Cabling

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

- The Power LED is green when the modem router is turned on.
- The LAN ports are green for each PC cabled to the router by an Ethernet cable.
- The wireless LED is green when the modem router is turned on.
- The DSL LED is green when you have a DSL connection.
- The Internet LED is red when there is no Internet connection.

Turn on your computer. If software usually logs you in to your Internet connection, do not run that software. If log-in software starts, cancel it.

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

Router Internet Setup

2

Connect to the Internet

This chapter explains three ways to set up your Internet connection: NETGEAR Genie (recommended), Setup Wizard, or manual setup. If you have already set up your router with one of these methods, the initial router setup is complete. You can read this chapter to become familiar with the router menus, to view or adjust the initial settings, or to change the router password and login time-out.

This chapter contains the following sections:

Router Setup Preparation

You can set up your wireless modem router with the NETGEAR Genie as described in *NETGEAR Genie Setup* on page 19, with the Setup Wizard as described in *Setup Wizard* on page 24, or manually as described in *Manual Setup (Basic Settings)* on page 25. However, before you start the setup process, have your ISP information on hand and ensure the laptops, PCs, and other devices in the network have the settings described here.

> **Note:** If you have a Macintosh or Linux system, you have to use the manual setup method.

Use Standard TCP/IP Properties for DHCP

If you configured your computer to use a static IP address, you need to change the settings back so that it uses Dynamic Host Configuration Protocol (DHCP). See *Appendix A, Technical Specifications* for more information.

Replace an Existing Router

To replace an existing router, disconnect the router completely from your network and set it aside before starting the router setup.

Adapters and Security Settings

A wireless adapter is the wireless radio in your PC or laptop that lets the PC or laptop connect to a wireless network. Most PCs and laptops come with an adapter already installed, but if the adapter is outdated or slow, you can purchase a USB adapter to plug into a USB port.

It is important that you make sure that the wireless adapter in each computer in your wireless network supports the same security settings as the wireless modem router. See *Preset Security* on page 32 for information about the router's preconfigured security settings.

> **Note:** If you connect devices to your modem router with WPS as described in *Wi-Fi Protected Setup (WPS) Method* on page 35, those devices assume the security settings of the router.

Gather ISP Information

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

- Active Internet service provided by a DSL account
- The ISP configuration information for your DSL account
  - ISP login name and password
  - ISP Domain Name Server (DNS) addresses
  - Fixed or static IP address
  - Host and domain names
  - Depending on how your ISP set up your Internet account, you could need to know one or more of these settings for a manual setup:
    - Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters
    - Multiplexing method
    - Host and domain names

NETGEAR Genie Setup

NETGEAR Genie is on the *Resource CD* and runs on a PC that has Microsoft Windows 7, Windows Vista, Windows XP, or Windows 2000 with Service Pack 2 or later installed. NETGEAR Genie is the easiest way to set up the router because it automates many of the steps and verifies that those steps have been successfully completed. The setup process takes about 15 minutes to complete.

Before running the NETGEAR Genie on a corporate PC, check with your company's network support staff. Corporate network settings or virtual private network (VPN) client software might conflict with the default settings of a home router. If you are unsure about whether there might be a conflict, use a different computer.

➢ **To run NETGEAR Genie:**

1. Locate the DSL settings information (user name and password) provided by your ISP. Contact your ISP if you do not have your DSL user name and password.
2. Insert the *Resource CD* into your Windows PC.

   The CD starts and detects the language on your PC. You can select a different language if you prefer.

   Note: *If the CD does not start, go to the CD drive (under My Computer on Windows), browse the CD, and double-click on the*  *icon.*

3. When the Welcome screen displays, click **Setup** to start the Genie.
4. Follow the instructions to complete the setup.

   NETGEAR Genie checks your hardware setup and guides you through connecting the router to the Internet and adding computers to your network.

Your wireless modem router connects to the Internet when any of the computers connected to your network require access. When you launch a web browser to access the Internet, the router's Internet LED blinks to indicate ISP communication.

View or Change Settings

You can view or change the settings in the following ways:

- Log in to your router by clicking the desktop shortcut that was placed on your desktop during the NETGEAR Genie setup. The shortcut icon is put on your desktop only when you use the NETGEAR Genie setup method.
- Log in to your router. See *Log In to the N150 Modem Router* on page 21.
- Open the Router_Setup.html file that was placed on your desktop during the NETGEAR Genie setup. This file provides setup and system information, the NETGEAR Technical Support number, links to the NETGEAR website, and a router login link.

Settings Description

When the NETGEAR Genie setup is completed, your router has the following configuration and informational settings. Some of these settings can be viewed in Router_Setup.html.

Configuration

- Wireless settings. The preconfigured Wi-Fi network name (SSID), passphrase, and security option (encryption protocol). See *Preset Security* on page 32 for more information.
- Internet connection including language and country as described in *Setup Wizard* on page 24.
- WAN port settings. This is your port address type (PPPoE by default) and ISP login name and password. See *Manual Setup (Basic Settings)* on page 25 for more information about address types.

Login and System Information

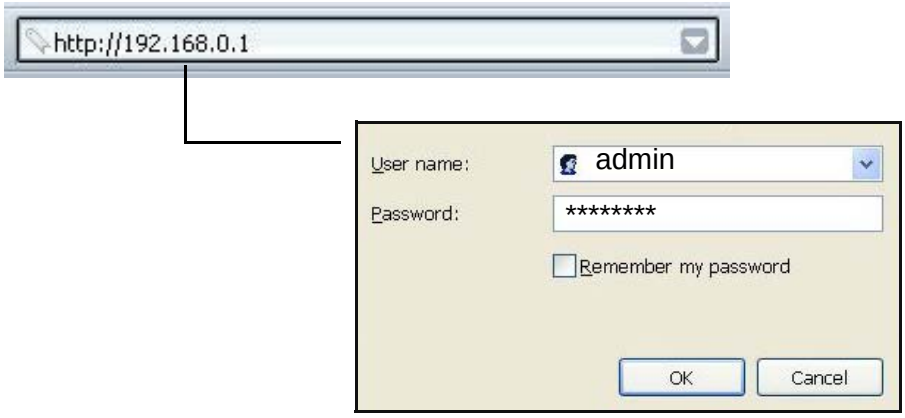
- Router login. The router administrator login name and password as described in *Log In to the N150 Modem Router* on page 21.
- System information. PC operating system, router serial number, and WAN Port MAC Address. See *Restrict Access by MAC Address* on page 33 for more information about MAC addresses.

Log In to the N150 Modem Router

Log in to the wireless modem router to view or change settings or to set up the wireless modem router.

➢ **To log in:**

1. Type **http://192.168.0.1** in the address field of your browser and press **Enter** to display the login window. You can also enter either of these addresses to access the wireless modem router: **http://www.routerlogin.net** or **http://www.routerlogin.com**.



2. When prompted, enter **admin** for the router user name and **password** for the router password, both in lowercase letters.

> ***Note:*** The router user name and password are probably different from the user name and password for logging in to your Internet connection. See *Types of Logins* on page 30 for more information.

The router menus display where you can do things like change settings or add other devices to your network. See *Router Interface* on page 23 for a brief description of the available functionality, and *Wi-Fi Protected Setup (WPS) Method* on page 35 for information about adding devices to your network.

If you do not see the login prompt:

1. Check the LEDs on the router front panel to make sure that the modem router is plugged into an electrical outlet, its power is on, and the Ethernet cable between your computer and the router is connected to a LAN port.
2. If you connected the Ethernet cable, quickly launched your browser, and typed in the router URL, your computer might need a minute or two to recognize the LAN connection. Relaunch your browser and try again.
3. If you are having trouble accessing the router wirelessly, use an Ethernet cable to connect your computer during setup so that you can log in to the wireless modem router.

Note: If you cannot connect to the wireless router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain both IP and DNS server addresses automatically. See your computer documentation for more information.

Upgrade Router Firmware

When you log in and if you are connected to the Internet, the Firmware Upgrade Assistant screen displays so you can upgrade to the latest available firmware. See *Chapter 5, Network Maintenance*, for more information about upgrading firmware.

1. Click **Yes** to check for new firmware (recommended). The modem router checks the NETGEAR database for new firmware.
2. If no new firmware is available, click **No** to exit. You can check for new firmware later.
3. If new firmware is available, click **Yes** to upgrade the router with the latest firmware. After the upgrade, the router restarts.

CAUTION:

Do not try to go online, turn off the router, shut down the computer, or do anything else to the router until the router finishes restarting and the Ready light has stopped blinking for several seconds.

You cannot upgrade firmware until you have established your Internet connection as described in *Setup Wizard* on page 24.

Router Interface

The router interface gives you access to the router's current settings so you can view or change them (if needed). The left column has the router menus, and the right column provides online help. The middle column is the screen for the current menu option.

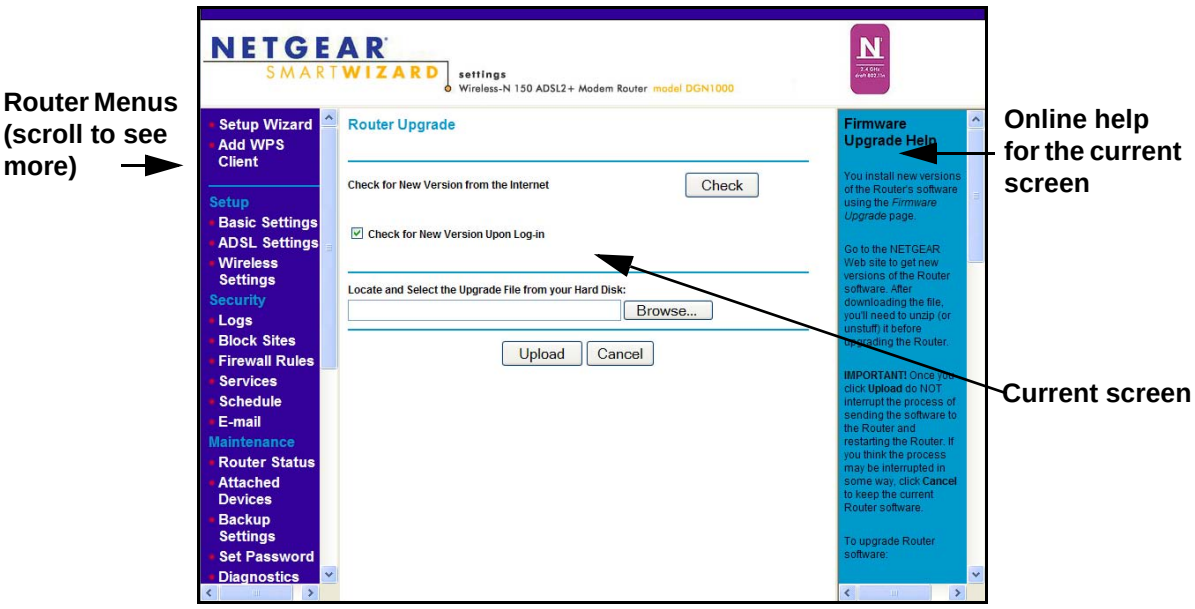


Figure 8. Router menus, Basic Settings screen, and online help

- **Setup Wizard**. Specify the language, location, and automatically detect the Internet connection. See *Setup Wizard* on page 24.
- **Add WPS Client**. Add WPS-compatible wireless devices and other equipment to your wireless network. See *Add Clients (Devices) to Your Network* on page 35.
- **Setup Menu**. Set, upgrade, and check the ISP and wireless network settings of your router. See *Manual Setup (Basic Settings)* on page 25 and *DSL Settings* on page 28. See also *Chapter 3, Wireless Settings*, for information about preset and basic security settings.
- **Security Menu**. View and configure the router firewall settings to prevent objectionable content from reaching your PCs. See *Chapter 4, Security Settings*.
- **Maintenance Menu**. Administer and maintain your router and network. See *Chapter 5, Network Maintenance*.
- **Advanced Menu**. Set the router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 6, Advanced Settings*. Using this menu requires a solid understanding of networking concepts.
- **Web Support**. Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

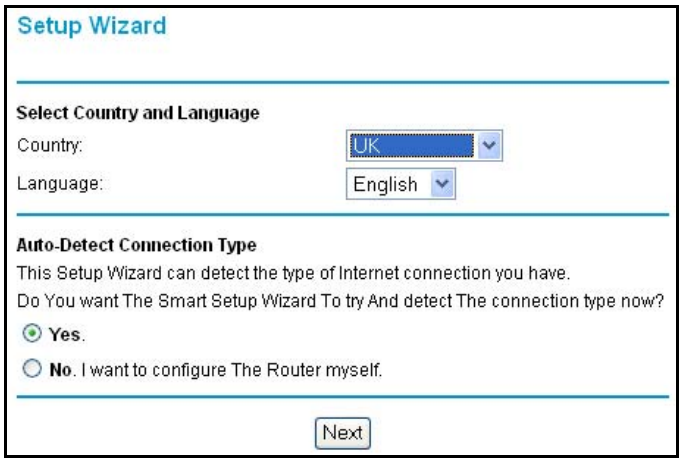
Setup Wizard

If you do not use the NETGEAR Genie, you have to log in to the modem router to set the country, language, and Internet connection.

> ***Note:*** If you performed the NETGEAR Genie setup, the country, language, Internet, and wireless network settings are already configured.

➢ **To run the Setup Wizard**

1. Select **Setup Wizard** from the top of the router menus to display the following screen:



2. Select your country and language:

- **Country**. It is important to specify the location where the wireless modem router operates so that the Internet connection works correctly. Defaults to UK.
- **Language**. Defaults to English. You can select another language if you prefer.

3. Select either **Yes** or **No, I want to configure the Router myself**. If you select No, proceed to *Manual Setup (Basic Settings)* on page 25.

4. If you selected Yes, click **Next**.

With automatic Internet detection, the Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

> ***Note:*** The Setup Wizard cannot detect a Point-to-Point Tunneling Protocol (PPTP) connection. If your ISP uses PPTP, you have to set your Internet connection through the screen described in *Manual Setup (Basic Settings)* described on 25.

Manual Setup (Basic Settings)

The Basic Settings screen displays when you select No. I want to configure the Router myself in the Setup Wizard and is also available from the router menus. It is where you view or change ISP information. The fields that display vary depending on whether or not your Internet connection requires a login.

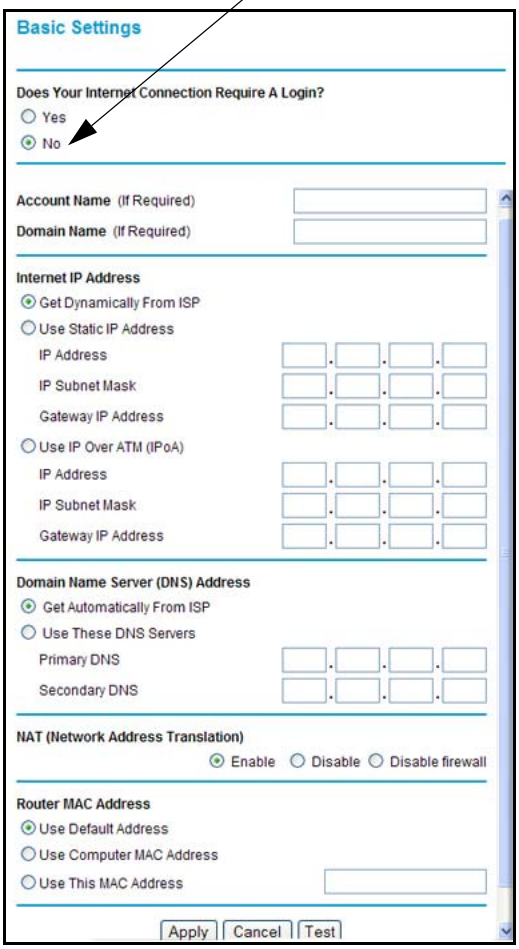
> ***Note:*** Check that the country and language are set as described *Setup Wizard* on page 24 before proceeding with the manual setup.

➢ **To perform a manual setup:**

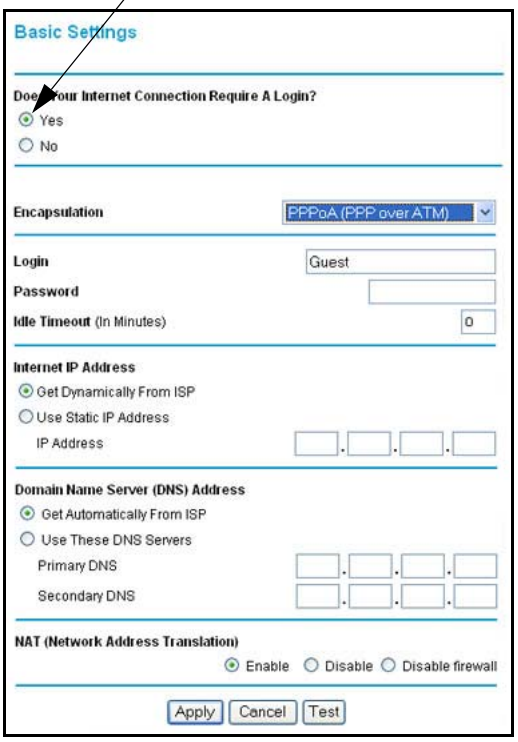
1. Select **Set Up > Basic Settings** and select **Yes** or **No** depending on whether or not your ISP requires a login. The following Basic Settings screens show both forms of the Basic Settings screen.
   - **Yes**. Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. Enter the account and domain names, as needed.
2. Enter the settings for the IP address and DNS server. The default DSL settings usually work fine. If you have problems with your connection, check the DSL settings and see *DSL Settings* on page 28 for more information.
3. If no login is required, you can specify the MAC Address setting.
4. Click **Apply** to save your settings.

5. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within 1 minute, see *Troubleshooting* on page 85.

ISP *does not* require login



ISP *does* require login



The following descriptions explain all of the possible fields in the Basic Settings screen. Note that which fields appear in this screen depends on whether or not an ISP login is required.

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

- *When no login is required, these fields display*:

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

  Domain Name (If required). Enter the domain name provided by your ISP.

- *When your ISP requires a login, these fields display*:

  Encapsulation. Encapsulation is a method for enclosing multiple protocols. PPP stands for Point-to-Point Protocol. The choices are PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM).

  Login. The login name provided by your ISP. This is often an email address.

Password. The password that you use to log in to your ISP.

Idle Timeout (In minutes). If you want to change the login timeout, enter a new value in minutes. This determines how long the wireless modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- *When a login is required, these fields display*:

  Get Dynamically from ISP. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.

  Use Static IP Address. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's wireless modem router to which your wireless modem router will connect.

- *When a login is not required, this field displays*:

  Use IP Over ATM (IPoA). Your ISP uses classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned.

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

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

Use These DNS Servers. If you know that your ISP does not automatically transmit DNS addresses to the wireless modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

NAT (Network Address Translation). NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices.

Enable. Usually NAT is enabled.

Disable. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure you do not need it. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses that the wireless modem router uses. Classical routing should be selected only by experienced users.[1]

Disable firewall. This disables the firewall in addition to disabling NAT. With the firewall disabled, the protections usually provided to your network are disabled.

When no login is required, this field displays:

Router MAC Address. The Ethernet MAC address used by the wireless modem router on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC

1. Disabling NAT reboots the wireless modem router and resets its configuration settings to the factory defaults. Disable NAT only if you plan to set up the wireless modem router in a setting where you will be manually administering the IP address space on the LAN side of the router.

address of that computer. This feature allows your wireless modem router to use your computer's MAC address (this is also called cloning).

Use Default Address. Use the default MAC address.

Use Computer MAC Address. The wireless modem router will capture and use the MAC address of the computer that you are now using. You need to be using the one computer that is allowed by the ISP.

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

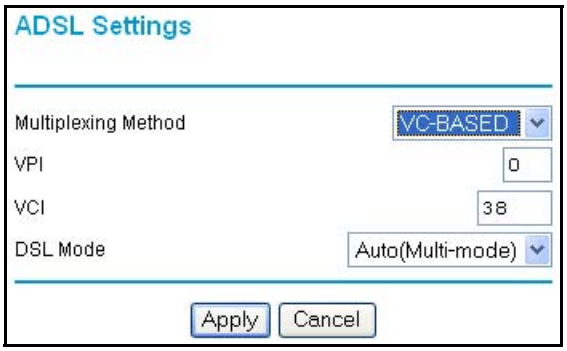
DSL Settings

The DSL settings of your wireless modem router work fine for most ISPs. However, some ISPs use a specific multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI).

Note: It is required that you use the Setup Wizard to select the correct country for the default DSL settings to work.

- **If your ISP gave you a multiplexing method or VPI/VCI number, enter the setting:**

1. Select **Setup > ADSL Settings** to display the following screen:



2. In the **Multiplexing Method** drop-down list, select **LLC-based** or **VC-based**.
3. For the VPI, type a number between 0 and 255. The default is 8 for the U.S. version, 0 for the world wide version, and 1 for the German version.
4. For the VCI, type a number between 32 and 65535. The default is 35 for the U.S. version, 38 for the worldwide version, and 32 for the German version.
5. Click **Apply**.

Unsuccessful Internet Connection

If you cannot connect to the Internet, you can do one or more of the following:

- Review your settings to be sure you have selected the correct options and typed everything correctly.
- Contact your ISP to verify that you have the correct configuration information.
- Read *Chapter 7, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR Technical Support.
- Check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain *both* IP and DNS server addresses automatically. See your computer documentation for more information.

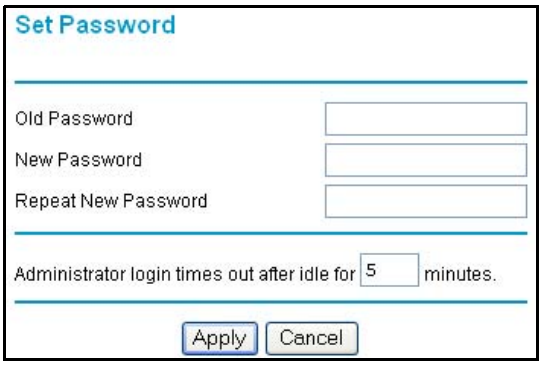
Change Password and Login Time-Out

For security reasons, the wireless modem router has its own user name and password that default to **admin** and **password**. You can and should change these to a secure user name and password that are easy to remember. The ideal password contains no dictionary words from any language and is a mixture of upper case and lower case letters, numbers, and symbols. It can be up to 30 characters.

Note: The router user name and password are not the same as the user name and password for logging in to your Internet connection. See *Types of Logins* on page 30 for more information about login types.

➢ **To change your password and login time-out:**

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



2. Enter the old password, and then enter the new password twice.
3. Change the login time-out to a value between 1 and 99 minutes if the default value of 5 minutes does not meet your needs.

The administrator's login to the wireless modem router configuration times out after a period of inactivity to prevent someone else from accessing the router interface when you step away.

4. Click **Apply** to save your changes.

   After changing the password, you are required to log in again to continue the configuration. If you have backed up the wireless modem router settings previously, you should do a new backup so that the saved settings file includes the new password. See *Back Up* on page 64 for information about backing up your network configuration.

Log Out Manually

The router interface provides a Logout command at the bottom of the router menus. Log out when you expect to be away from your computer for a relatively long period of time.

➢ **To log out manually:**

Click Log Out at the bottom of the router menus.

Types of Logins

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

- **Router login** logs you in to the router interface. See *Log In to the N150 Modem Router* on page 21 for details about this login.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wi-Fi network name and passphrase** logs you in to your wireless network. This login is preconfigured and can be found on the label on the bottom of your unit. See *Chapter 3, Wireless Settings*, for more information.

Wireless Settings

3

Protect your network

This chapter describes how to use the Wireless Settings screens to view and change (if needed) your wireless network settings. Security features to prevent objectionable content from reaching your PCs are covered in *Chapter 4, Security Settings*.

This chapter contains the following sections:

Preset Security

The N150 Modem Router comes with preset security. This means that the Wi-Fi network name (SSID), passphrase, and security option (encryption protocol) are preset in the factory. You can find the preset SSID and passphrase on the bottom of the unit.

- **Wi-Fi network name (SSID)** identifies your network so devices can find it.
- **Passphrase** controls access to your network. Devices that know the SSID and the passphrase can find your wireless network and connect.

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

- **Security option** is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. The preset security option is WPA-PSK/WPA2-PSK mixed mode described in *Wireless Security Options* on page 33.

The Wireless Settings screen lets you view and change the preset security settings. ***However, it is important to understand that NETGEAR recommends that you not change your preset security settings***. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

Security Basics

Unlike wired network data, wireless data transmissions extend beyond your walls and can be received by any device with a compatible wireless adapter (radio). For this reason, it is very important to maintain the preset security and understand the other security features available to you. Besides the preset security settings described above, your wireless modem router has the security features described here and in *Chapter 4, Security Settings*.

- Turn off wireless connectivity
- Disable SSID broadcast
- Restrict access by MAC address
- Wireless security options

Turn Off Wireless Connectivity

You can completely turn off the wireless connectivity of the wireless modem router by pressing the Wireless On/Off button on its front panel  . For example, if you use your notebook computer to wirelessly connect to your wireless modem router and you take a business trip, you can turn off the wireless portion of the modem router while you are traveling. Other members of your household who use computers connected to the wireless modem router through Ethernet cables can still use the wireless modem router.

Disable SSID Broadcast

By default, the wireless modem router broadcasts its Wi-Fi network name (SSID) so devices can find it. If you change this setting to not allow the broadcast, wireless devices will not find your wireless modem router unless they are configured with the same SSID. See *Wireless Access Point Settings* on page 39 for the procedure.

> ***Note:*** Turning off SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. If you allow the broadcast, be sure to keep wireless security enabled.

Restrict Access by MAC Address

You can enhance your network security by allowing access to only specific PCs based on their Media Access Control (MAC) addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the wireless modem router. MAC address filtering adds additional security protection to the wireless security option you have in force. The Wireless Station Access List determines which wireless hardware devices are allowed to connect to the wireless modem router by MAC address. See *Wireless Station Access List Settings.* on page 39 for the procedure.

Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are two types of encryption: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WPA is stronger, and therefore, recommended over WEP. WPA has several options including pre-shared key (PSK) encryption and 802.1x encryption for enterprises.

This section presents an overview of the security options and provides guidance on when to use which option. Note that it is also possible to disable wireless security. NETGEAR does *not* recommend this.

WEP Encryption

WEP uses an old encryption method and can be easily decoded with today's powerful computers. Use this mode only when you have a very old legacy wireless client that does not support WPA-PSK. The Wi-Fi alliance highly recommends against using WEP and plans to make it obsolete. If you do decide to use WEP, see *Set WEP Encryption and Passphrase* on page 42 for the procedure.

WPA Encryption

WPA encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means the product is authorized by the Wi-Fi Alliance (*http://www.wi-fi.org/*) because it complies with the worldwide single standard for high-speed wireless local area networking. For information about how to use the WPA home options, see *Change WPA Security Option and Passphrase* on page 41.

- WPA-PSK uses a much stronger encryption algorithm than WEP so it is harder to decode. This option uses a passphrase to perform the authentication and generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption, implements most of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards, but not all wireless access points. It is superseded by WPA2-PSK.
- WPA2-PSK is the strongest. It is advertised to be theoretically indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is usually implemented through hardware, while WPA-PSK is usually implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.
- WPS-PSK + WPA2-PSK Mixed Mode is the preconfigured security mode on the wireless modem router. NETGEAR recommends mixed mode because it provides broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. The product documentation for your wireless adapter and WPA client software should have instructions about configuring their WPA settings.
- WPA-802.1x is enterprise-level security and requires an authentication server to recognize and authorize client access. The authentication server is called Remote Authentication Dial In User Service (RADIUS). Every wireless client has a user login on the RADIUS server, and the wireless modem router has a client login on the RADIUS server. Data transmissions are encrypted with an automatically generated key. For information about how to use the WPA enterprise option, see *Set WPA-802.1x Server and Passphrase* on page 41.

Add Clients (Devices) to Your Network

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

Manual Method

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

Wi-Fi Protected Setup (WPS) Method

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

> **Note:** If you find that the router is generating new security settings for each added device, it means that the default value for Keep Existing Wireless Settings has changed. See *WPS Settings.* on page 79 for more information about this setting.

All Wi-Fi-certified and WPS-capable products are compatible with the NETGEAR products that have Push 'N' Connect, which is based on WPS[1]. For information about how to view a list of all wireless and wired devices connected to your modem router, see *View Attached Devices* on page 70.

> **Note:** WEP security does not support WPS. If you try to use WPS to connect a WEP device to your network, it will not connect.

You can use the WPS (Push 'N' Connect) or router interface method to add wireless devices and other equipment to your wireless network.

1. For a list of other Wi-Fi-certified products available from NETGEAR, go to http://www.wi-fi.org.

WPS (Push 'N' Connect) Method

If your wireless device supports WPS (Push 'N' Connect), you can use WPS.

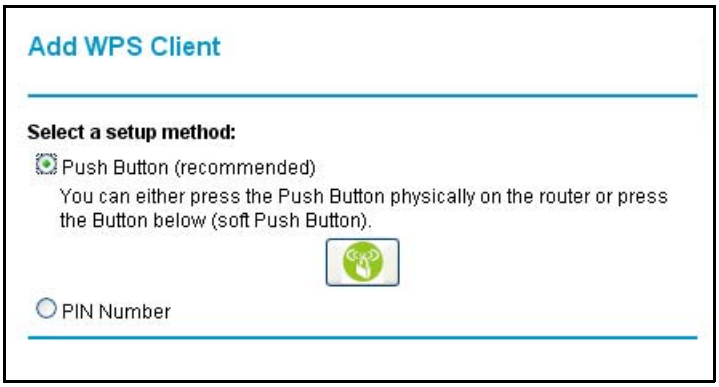
➢ **To use WPS:**

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

Router Interface Method

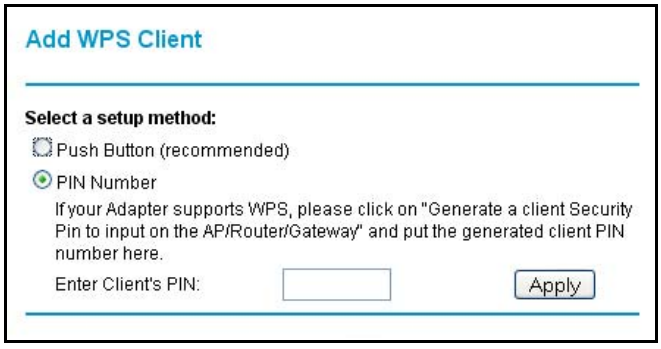
➢ **To use the router interface method:**

1. Select **Add WPS Client** at the top of the router menus. If you cannot select Add WPS Client, select **Setup > Wireless Settings** and make sure WPS is selected.
2. Click **Next**. The following screen lets you select the method for adding the WPS client.



3. Select either **Push Button** or **PIN Number**. With either method, the client wireless device attempts to detect the WPS signal from the wireless modem router and establish a wireless connection in the time allotted.

   The PIN method displays this screen so you can enter the client security PIN number:



   - While the wireless modem router attempts to connect to a WPS-capable device, the WPS LED on the front of the wireless modem router blinks green. When the wireless modem router establishes a WPS connection, the LED is solid green.

- If a connection is established, the wireless modem router WPS screen displays a confirmation message.

4. Repeat to add another WPS client to your network.

Wireless Settings Screen

The Wireless Settings screen lets you view or configure the wireless network configuration. If you want to make changes, note the current settings first. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs. ***NETGEAR recommends that you not change the Wi-Fi network name (SSID), WPA/WPA2-PAK passphrase, or security option,*** but if you want to change these settings, this section explains how.

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

Consider Every Device on Your Network

Before you begin, check the following:

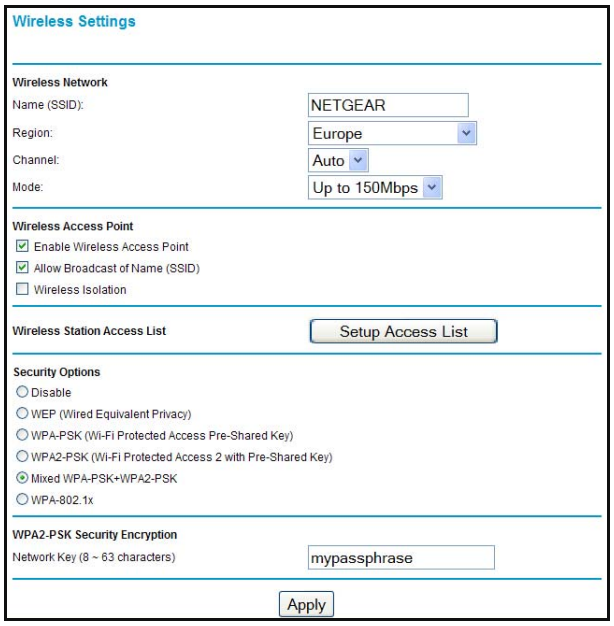
- Every wireless computer has to be able to obtain an IP address by DHCP from the router as described in *Use Standard TCP/IP Properties for DHCP* on page 18.
- Each computer or wireless adapter in your network is required to have the same SSID and wireless mode (bandwidth/data rate) as the router. Check that the wireless adapter on each computer can support the mode and security option you want to use.
- The security option on each wireless device in the network is required to match the router. For example, if you select a security option that requires a passphrase, be sure to use same passphrase for each wireless computer in the network.

View or Change Wireless Settings

Your preset router comes set up with a unique wireless network name (SSID) and network password. This information is printed on the label for your router. You can view or change these settings in the Wireless Settings screen.

➢ **To change the wireless settings:**

1. Select **Setup > Wireless Settings** to display the following screen.



2. Make any changes that are needed and click **Apply** when done to save your settings.

> ***Note:*** The screen sections, settings, and procedures are explained in the following sections.

3. After you finish adjusting settings and click Apply, configure and test your computers for wireless connectivity:
   a. Program the wireless adapter of your computers to have the same SSID and channel that you specified in the router.
   b. Check that the adapters have a wireless link and can obtain an IP address by DHCP from the wireless modem router.

Wireless Network Settings

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and ***NETGEAR strongly recommends that you not change this***.

Region. The location where the wireless modem router is used. It might not be legal to operate the wireless modem router in a region other than the regions listed.

Channel. The wireless channel used by the gateway: 1 through 13. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

Mode. Up to 150 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. Up to 65 Mbps supports up to 65 Mbps.

Wireless Access Point Settings

Enable. When this check box is not selected, the wireless signal in the router so it can accept wireless clients. When not enabled, the router accepts wired clients only. This check box is selected by default.

Allow Broadcast of Name (SSID). This setting allows the wireless modem router to broadcasts its SSID so wireless stations can see this wireless name (SSID) in its scanned network list. This check box is selected by default. To turn off the SSID broadcast, clear the **Allow Broadcast of Name (SSID)** check box and click **Apply**.

Wireless Isolation. When this check box is selected, wireless stations cannot communicate with each other or with stations on the wired network. This check box is not selected by default.

Wireless Station Access List Settings.

The Wireless Stations Access List lets you restrict access to your network to a specific list of devices based on their MAC addresses.

➢ **To set up a WIreless Station Access list.**

1. On the Wireless Settings screen, click the **Setup Access List** button to display the Wireless Station Access List screen shown next and introduced here:
   - The Turn Access Control On check box at the top is not selected by default to allow any computer configured with the correct wireless network name (SSID) and passphrase to access the network.
   - Trusted Wireless Stations lists the trusted computers that have access to your network.
   - Available Wireless Stations lists the currently untrusted computers that are connected to your network.

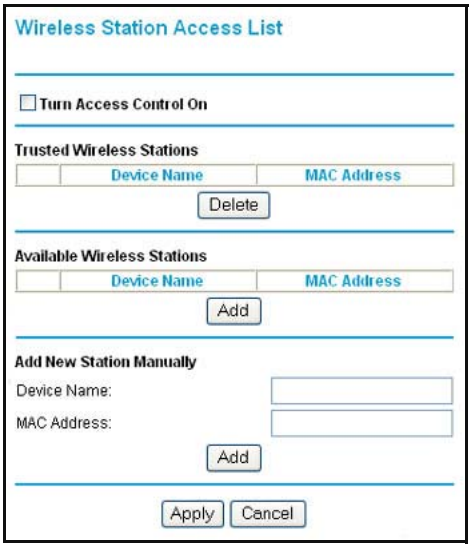


Figure 9. Wireless Station Access List

2. Select the **Turn Access Control On** check box to enable access restriction by MAC address.
3. In the Add New Station Manually list, click **Add** to add your computer's MAC address so you do not lose your wireless connection when you click Apply. If you lose your wireless connection, you have to access the wireless modem router from a wired computer or from a wireless computer that is on the access control list.
4. If a wireless station that you want to add to the Trusted Wireless Stations list is connected to the network, select it from the Available Wireless Stations list and click **Add**.
5. If the wireless station is not currently connected, you can enter its address manually. The MAC address is usually printed on the wireless card, or it might appear in the wireless modem router's DHCP table. The MAC address is 12 hexadecimal digits.

   You can also copy and paste the MAC addresses from the wireless modem router's Attached Devices screen (see *View Attached Devices* on page 70) into the MAC Address field. To do this, configure each wireless computer to obtain a wireless link to the wireless modem router. The computer should then appear in the Attached Devices screen.
6. Click **Apply** to save your settings and return to the Wireless Settings screen.

Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. See *Wireless Security Options* on page 33 for an explanation of the security options and when to use which one. Please note that ***NETGEAR recommends that you not change the security option or passphrase,*** but if you want to change these settings, this section explains how. ***Do not disable security***.

Change WPA Security Option and Passphrase

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

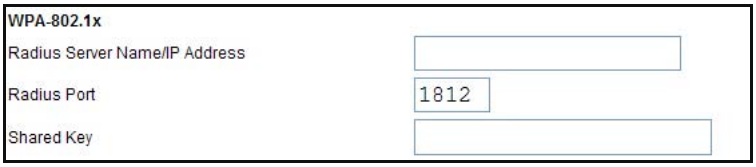
1. In the Security Options section, select the WPA option you want.

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

Set WPA-802.1x Server and Passphrase

➢ **To set the WPA-802.1x server and passphrase:**

1. In the Security Options section, select **WPA-802.1x** to display the following fields:



2. In the Radius Server Name/IP Address field, enter the name or IP address of the RADIUS server on your LAN. This is a required field.
3. In the Radius Port field, enter the port number used for connections to the RADIUS server. The default port is 1812.
4. In the Shared Key field, enter the RADIUS server passphrase for client logins. The router has to have this passphrase to log into the RADIUS server as a client.

Set WEP Encryption and Passphrase

When configuring WEP from a wireless computer, you lose your wireless connection when you click Apply. You have to either configure your wireless adapter to match the wireless modem router WEP settings or access the wireless modem router from a wired computer.

➢ **To set WEP encryption and passphrase:**

1. In the Security Options section, select **WEP** to display the following screen:

2. Select the authentication type. The default is Automatic. Other choices are Open System (any client can authenticate itself to the network) and Shared Key (a passphrase and a four-way challenge is needed for authentication).
3. Select the encryption strength setting, either 64 bit or 128 bit.
4. Enter the four data encryption keys either manually or automatically. These values are required to be identical on all computers and access points in your network.
   - Automatic. Enter a word or group of printable characters in the Passphrase field and click Generate. The four key fields are automatically populated with key values.
   - Manual. The number of hexadecimal digits that you enter depends on the encryption strength setting:
     - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
     - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
5. Select the radio button for the key you want to make active.

   Make sure you understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one in Windows XP allow one key entry, which has to match the default key you set in the wireless modem router.
6. Click **Save** to save your settings or click **Apply** so your changes to take effect immediately.

Security Settings

4

Keep unwanted content out of your network

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

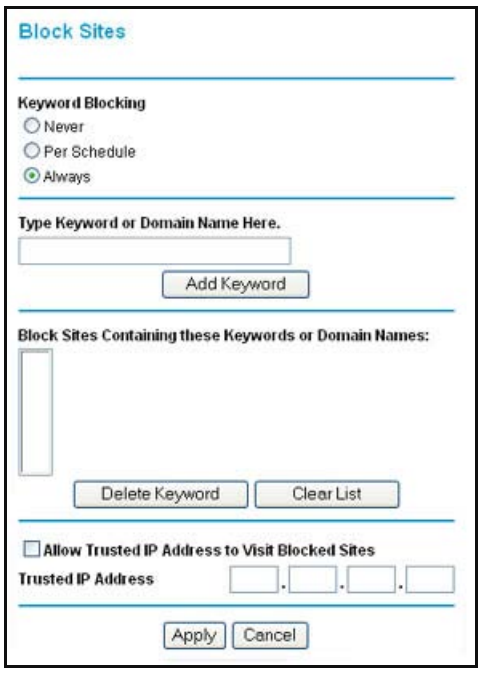
This chapter contains the following sections:

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 scheduled.

➢ **To block by keywords:**

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



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.

Delete a Keyword or Domain

➢ **To delete a keyword or domain:**

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

Specify a Trusted Computer

You can exempt one trusted computer from blocking and logging. That computer has to be configured to use a a fixed IP address.

➢ **To specify a trusted computer:**

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

Firewall Rules to Control Network Access

By default your router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. You might need to create exceptions to this rule to allow remote computers to access a server on your local network or to allow certain applications and games to work correctly. Your router provides firewall rules for creating these exceptions.

Authorized communications are established according to inbound and outbound rules. The firewall has the following two default rules. You can create custom rules to further restrict the outbound communications or more widely open the inbound communications:

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

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.

Open Inbound Ports (Port Forwarding)

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.By using the inbound rule 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. WIth inbound rules, 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 inbound 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 inbound rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (for example, port 33333) as the destination port. The IRC server also sends an identify message to your router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your router checks its session table 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 inbound rules, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application, or the relevent user groups or newsgroups.

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

Inbound Rules 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 inbound rules feature.

A typical application of inbound rules 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. By using inbound rules, 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 inbound 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 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 inbound 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 inbound rules, 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/or newsgroups.

How Inbound Rules Differ from Outbound Rules

The following points summarize the differences between inbound rules and outbound rules:

- Outbound rules can be used by any computer on your network, although only one computer can use them at a time.
- Inbound rules are configured for a single computer on your network.
- Outbound rules do not need to know the computer's IP address in advance. The IP address is captured automatically.
- Inbound rules require that you specify the computer's IP address during configuration, and the IP address can never change.
- Outbound rules require specific outbound traffic to open the inbound ports, and the outbound ports are closed after a period of no activity.
- Inbound Rules are always active and do not need to be made active.

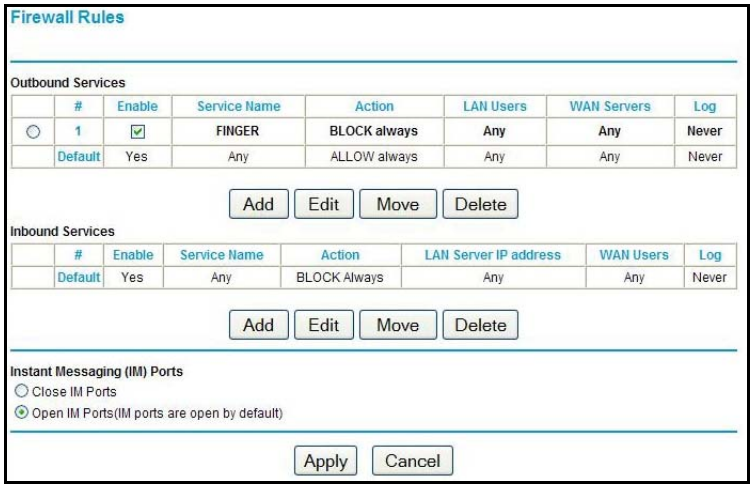
Configure Firewall Rules

The Firewall Rules screen lets you configure custom rules to make exceptions to the default rules. Exceptions can be based on the service or application, source or destination IP addresses, and time of day. You can log traffic that matches or does not match the rule and change the order of rule precedence. See *Configure Services* on page 54 for information about services.

All traffic attempting to pass through the firewall is subjected to the rules in the order shown in the Rules table from the top (highest precedence) to the default rules at the bottom. In some cases, the order of precedence is important to determine which communications are allowed into or out of the network.

➢ **To configure firewall rules:**

1. Select **Security > Firewall Rules** to display the following screen:



2. To add an inbound or outbound rule:
   - For an outbound rule, click **Add** under Outbound Services.

- For an inbound rule, click **Add** under Inbound Services.

3. To edit or delete a rule, select its button on the left side and click **Edit** or **Delete**.
4. To change the order of precedence:
   a. Select its button on the left side of the table and click **Move**.
   b. At the prompt, enter the number of the new position and click **OK**.
5. To open or close instant messaging, select a radio button: and click **Apply**.
   - **Close IM Ports**. Disables instant messaging traffic.
   - **Open IM Ports**. Enables instant messaging traffic. IM ports are open by default.
6. Click **Apply** to save your settings.

Inbound Rules (Port Forwarding)

Because the wireless modem router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet.

The rule tells the wireless modem router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding. Allowing inbound services opens holes in your firewall. Enable only those ports that are necessary for your network. The following are two examples of inbound rules.

> ***Note:*** Some residential broadband ISP accounts do not let you run server processes (such as a web or FTP server) from your location. Your ISP might periodically check for servers and suspend your account if it discovers any active services at your location. If you are unsure, refer to the acceptable use policy of your ISP.

Inbound Rule Example: A Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests from any outside IP address to the IP address of your web server at any time of day, as shown here and described in the following figure:

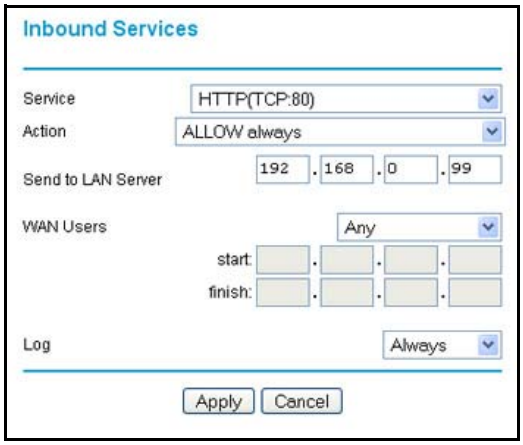


Figure 10. Allow inbound web requests

Service. From this list, select the application or service you want to allow or block. The list already displays many common services, but you are not limited to these choices. Use the Services screen to add any additional services or applications that do not already appear. See *Configure Services* on page 54.

Action. Choose how you want to handle this type of traffic. You can block or allow always, or you can block or allow according to the schedule you have defined in the Schedule screen, described in *Schedule Firewall Services* on page 57.

Send to LAN Server. Enter the IP address of the computer or server on your LAN that receives the inbound traffic covered by this rule.

WAN Users. These settings determine which packets are covered by the rule, based on their source (WAN) IP address:

Any. All IP addresses are covered by this rule.

Address range. When this option is selected, the **Start** and **Finish** fields are required.

Single address. Enter the required address in the **Start** field.

Log. You can select whether to log the traffic:

Never. No log entries are made for this service.

Always. Any traffic for this service type is logged.

Match. Traffic of this type that matches the settings and action are logged.

Not match. Traffic of this type that does not match the settings and action are logged.

Inbound Rule Example: Allowing Video Conferencing

Create an inbound rule to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office. In the following figure, CU-SeeMe connections are allowed from a specified range of external IP addresses only. In this case, logging of any incoming CU-SeeMe requests that do not match the allowed settings is always allowed.

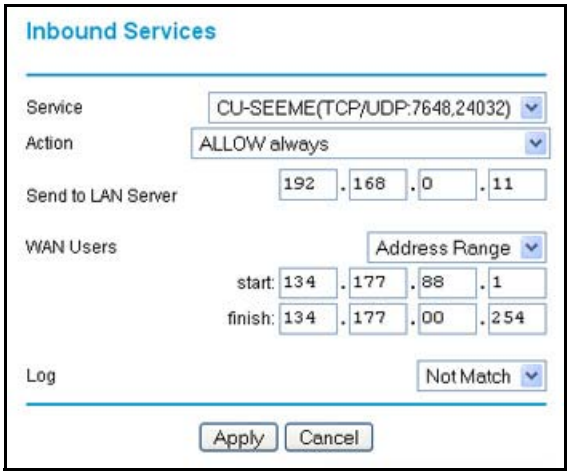


Figure 11. Allow inbound video conferencing

Considerations for Inbound Rules

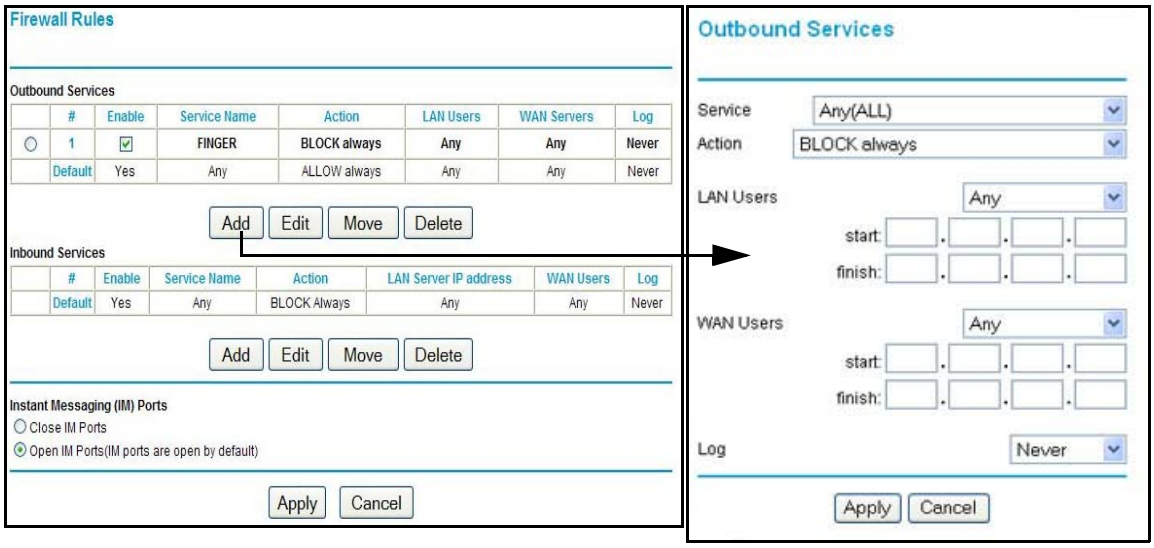
- If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS screen described in *Dynamic DNS* on page 75 so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP Setup screen to keep the computer's IP address constant.
- Local computers are required to access the local server using the computer's local LAN address (192.168.0.11 in the example shown in *Figure 11, Allow inbound video conferencing*). Attempts by local computers to access the server using the external WAN IP address fail.

Outbound Rules (Service Blocking)

The wireless modem router lets you block computers on your local network from using certain Internet services. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on local computer, Internet site being contacted, time of day, and type of service being requested.

➢ **To set up service blocking:**

1. Select **Security > Firewall Rules** to display the following screen:



2. Under Outbound Services, click **Add.**
3. Fill in the settings as follows and click **Apply** to save your settings.

Service. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the **Add Custom Service** button in the Services screen described in *Configure Services* on page 54 to add any additional services or applications that do not already appear.

Action. Choose how to handle this type of traffic. You can block or allow always, or you can block or allow according to the schedule you defined, as described in *Schedule Firewall Services* on page 57.

LAN Users. These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the option that you want:

Any. All IP addresses are covered by this rule.

Address range. If this option is selected, fill in the **Start** and **Finish** fields.

Single address. Enter the required address in the **Start** field.

WAN Users. These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the option that you want:

Any. All IP addresses are covered by this rule.

Address range. If this option is selected, fill in the **Start** and **Finish** fields.

Single address. Enter the required address in the **Start** field.

Log. You can select to log the traffic:

Never. No log entries are made for this service.

Always. Any traffic for this service type is logged.

Match. Traffic of this type that matches the settings and action is logged.

Not match. Traffic that does not match the settings and action are logged.

Configure Services

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 destination port number 80 is an HTTP (web server) request.

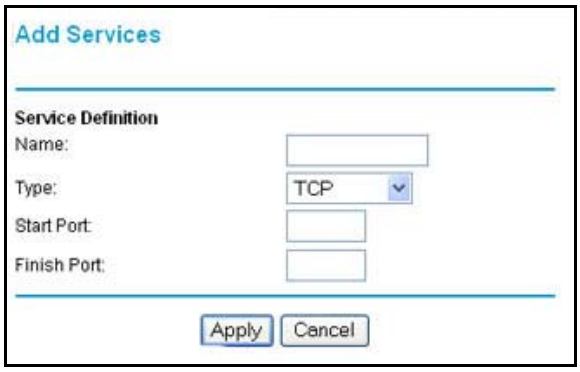
The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. Although the wireless modem router already holds a list of many service port numbers, you are not limited to these choices.

➢ **To create your own service definitions:**

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

- To create a new service, click the **Add Custom Service** button to display the Add Services screen.
- To edit a service, select its button on the left side of the table, and click **Edit Service**.
- To delete a service, select its button on the left side of the table, and click **Delete Service**.

2. Use the following screen to define or edit a service.



- **Name**. Enter a meaningful name for the service.
- **Type**. Select the correct type for this service. If in doubt, select **TCP/UDP**. The options are TCP, UDP, TCP/UDP.
- **Start Port** and **End Port**. If a port range is required, enter the range here. If a single port is required, enter the same value in both fields.

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

Set the Time Zone

The wireless modem router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. You can check and set (if needed) the time zone to ensure time stamps match your local time.

➢ **To set the time zone:**

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

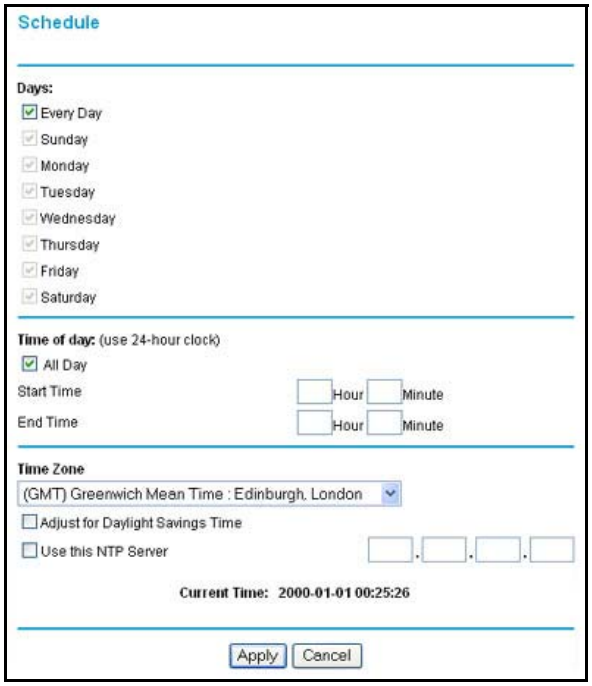


Figure 12. Time zone options

2. Select your time zone. This setting determines the blocking schedule and time-stamping of log entries.
3. If your time zone is in daylight savings time, select the **Adjust for Daylight Savings Time** check box to add one hour to standard time.

> ***Note:*** If your region uses daylight savings time, select Adjust for Daylight Savings Time on the first day and clear it after the last day.

4. The wireless modem router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, select the **Use this NTP Server** check box, and enter its IP address.
5. Click **Apply** to save your settings.

Schedule Firewall Services

If you enabled services blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

➢ **To schedule firewall services:**

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

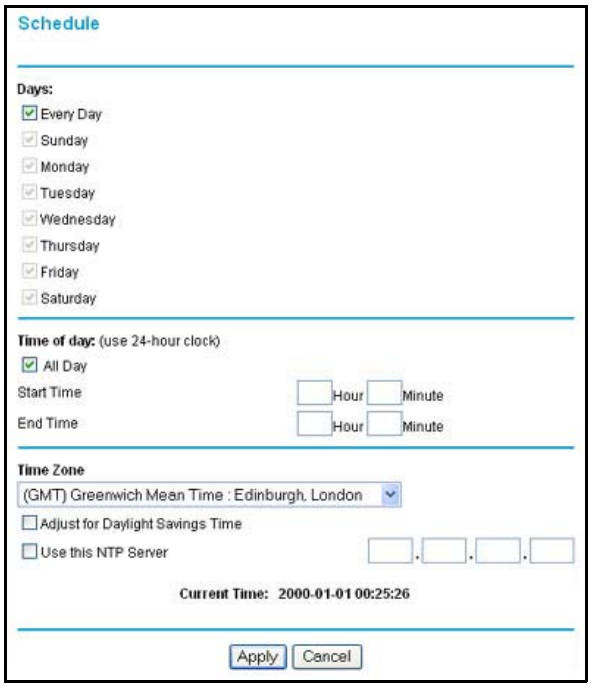


Figure 13. Block Internet services based on a schedule

2. To block Internet services based on a schedule, select **Every Day** or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, enter times in the **Start Time** and **End Time** fields.

Note: Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule is effective through midnight the next day.

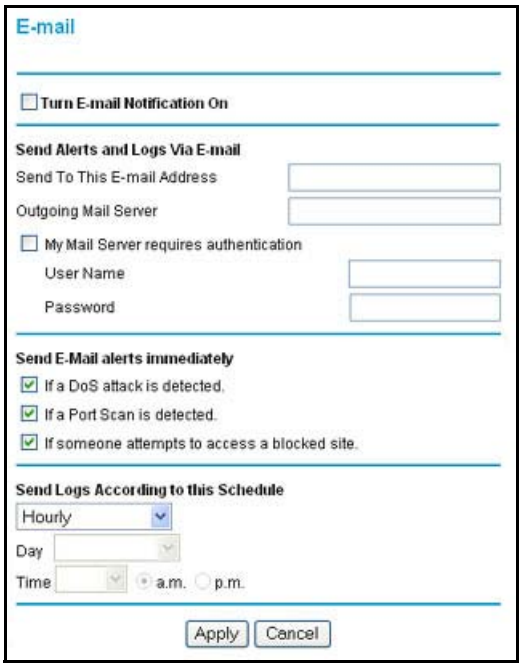
3. Click **Apply** to save your settings.

Enable Security Event Email Notification

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

➢ **To enable email notification:**

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



2. Fill in the fields as follows:

Turn E-mail Notification On. Select this check box if you want to receive email logs and alerts from the wireless modem router.

Send To This E-mail Address. Enter the email address where you want logs and alerts sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.

Outgoing Mail Server. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your email program. Enter the email address to which logs and alerts are sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by e-mail.

My Mail Server requires authentication. If you use an outgoing mail server provided by your current ISP, you do not need to select this field. If you use an email account that is not provided by your ISP, select this field, and enter the required user name and password information.

Send E-Mail alerts immediately. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.

Send Logs According to this Schedule. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.

Day for sending logs specifies which day of the week to send the log. This is relevant when the log is sent weekly.

Time for sending log specifies the time of day to send the log. This is relevant when the log is sent daily or weekly.

Note: If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, it is cleared from the wireless modem router's memory. If the wireless modem router cannot email the log file, the log buffer might fill up. In this case, the wireless modem router overwrites the log and discards its contents.

Network Maintenance

5

Administer your network

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

This chapter contains the following sections:

Upgrade the Router Firmware

The wireless modem router firmware (routing software) is stored in flash memory. By default, when you log in to your wireless modem router, it checks the NETGEAR website for new firmware and alerts you if there is a newer version.

WARNING:

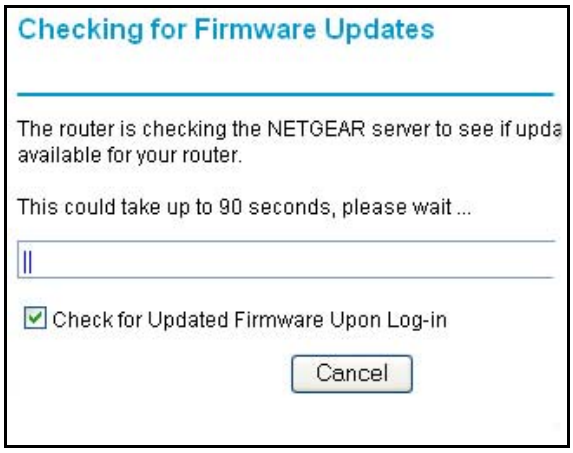
When uploading firmware to the wireless modem router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

Turn Off Automatic Firmware Checking

You can turn the automatic firmware checking off and check for firmware updates manually if you prefer. See *Manual Check for Firmware Upgrades* on page 63.

➢ **To turn off the automatic firmware check at log in:**

1. Select **Maintenance > Router Upgrade**.
2. Uncheck the **Check for Updated Firmware Upon Log-in** check box at the bottom of this screen:.



Automatic Firmware Checking On

When automatic firmware checking is on, the wireless modem router performs the check and notifies you if an upgrade is available or not as shown here.

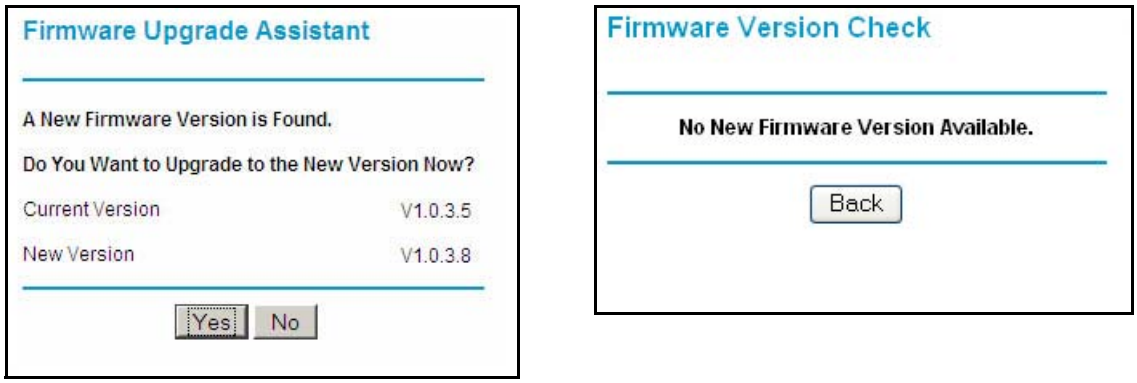


Figure 14. Firmware upgrade assistant and results screen

➢ **To upgrade the firmware:**

1. Click **Yes** to allow the wireless modem router to download and install the new firmware. The upgrade process could take a few minutes. When the upload is complete, your wireless modem router restarts.
2. Go to the DGN1000 support page at *http://support.netgear.com*and read the new firmware release notes to determine whether you need to reconfigure the modem router after upgrading.

Note: If you get a “Firmware needs to be reloaded” message, it means a problem has been detected with the router’s firmware. Follow the prompts to correct the problem or see *Firmware Needs to Be Reloaded* on page 93 for a description of the steps.

Manual Check for Firmware Upgrades

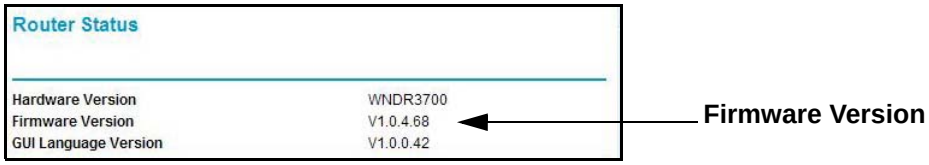
You can use the Router Upgrade screen to manually check the NETGEAR website for newer versions of firmware for your product.

WARNING:

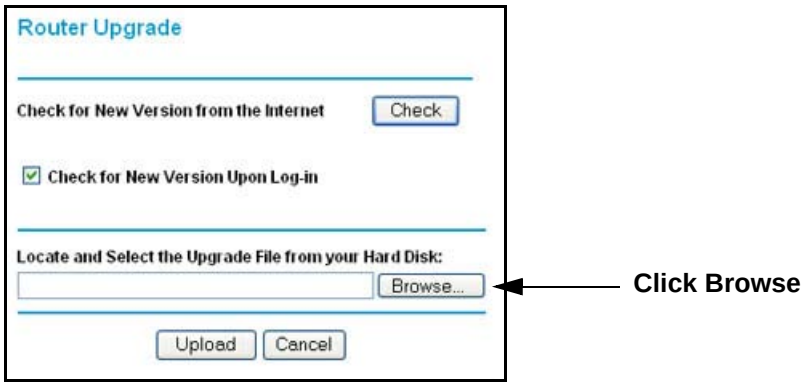
When you upload firmware to the router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

➢ **To check for firmware upgrades:**

1. Select **Maintenance > Router Status** and make a note of the wireless modem router firmware version number..



2. Go to the DGN1000 support page on the NETGEAR website at *http://www.netgear.com/support.*
3. If the firmware version on the NETGEAR website is newer than the firmware on your wireless modem router, download the file to your computer.
4. To upload the newer firmware, select **Maintenance > Router Upgrade** to display the following screen:



5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img).
6. Click **Upload** to send the firmware to the wireless modem router.

   When the upload completes, your wireless modem router restarts. The upgrade process typically takes about one minute. Read the new firmware release notes to determine whether or not you need to reconfigure the wireless modem router after upgrading.

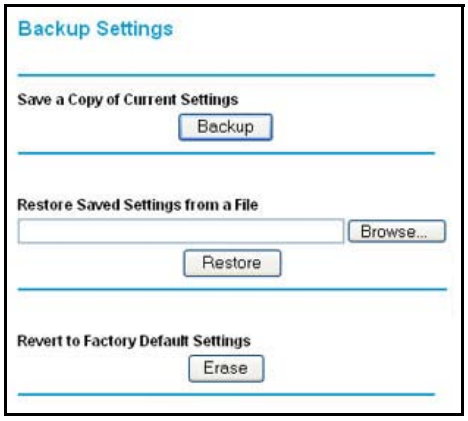
Manage the Configuration File

The router configuration settings are stored in a configuration file (*.cfg). This file can be backed up to your computer, restored, or reverted to factory default settings.

Back Up

➢ **To back up the configuration file:**

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



2. Click **Backup** 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

➢ **To restore the configuration file from backup:**

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 wireless modem router.

Upon completion, the wireless modem router reboots.

WARNING:

Do not interrupt the reboot process.

Erase

➢ **To erase the configuration and restore to factory defaults:**

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.

Click the **Erase** button to reset the wireless modem router to its factory default settings. Alternately, press the Wireless On/Off and WPS buttons on the side panel of the wireless modem router simultaneously for 6 seconds.

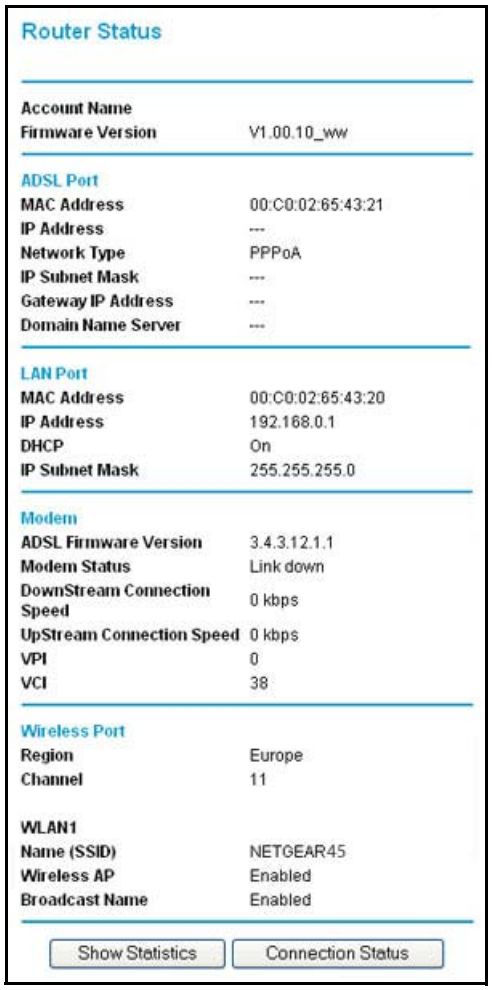
Erase sets the user name to admin, the password to password, the LAN IP address to 192.168.1.1, and enables the wireless modem router's DHCP.

To restore the factory default configuration settings when you do not know the login password or IP address, use the restore factory settings button on the bottom of the router (see *Factory Settings* on page 94).

View Router Status

➢ **To view the router status:**

1. Select **Maintenance > Router Status** to display the following screen. The Router Status screen provides the status and usage information described in the following figure.



2. Fill in the fields as follows:

Account Name. The host name assigned in the Basic Settings screen.

Firmware Version. The firmware version.

ADSL Port.

MAC Address. The Ethernet MAC address of the DSL port.

IP Address. The DSL port IP address. If no address is shown, the wireless modem router cannot connect to the Internet.

Network Type. The value depends on your ISP.

IP Subnet Mask. The DSL port IP subnet mask.

Gateway IP Address. The IP address used as a gateway to the Internet for computers configured to use DHCP.

Domain Name Server. The wireless modem router DNS server IP addresses. These addresses are usually obtained dynamically from the ISP.

LAN Port (Local Ports).

MAC Address. The wireless modem router LAN port Ethernet MAC address.

IP Address. The wireless modem router LAN port IP address. The default is 192.168.0.1.

DHCP. If Off, the wireless modem router does not assign IP addresses to PCs on the LAN. If On, the wireless modem router does assign IP addresses to PCs on the LAN.

IP Subnet Mask. The IP subnet mask used by the wireless modem router LAN. The default is 255.255.255.0.

Modem.

ADSL Firmware Version. The version of the firmware.

Modem Status. The connection status of the modem.

DownStream Connection Speed. The modem receives data from the DSL line at this speed.

UpStream Connection Speed. The modem transmits data to the DSL line at this speed.

VPI. The Virtual Path Identifier setting.

VCI. The Virtual Channel Identifier setting.

Wireless Port. See *Wireless Settings Screen* on page 37 for a description of these settings.

Name (SSID). The Wi-Fi network name (service set ID) for the wireless network.

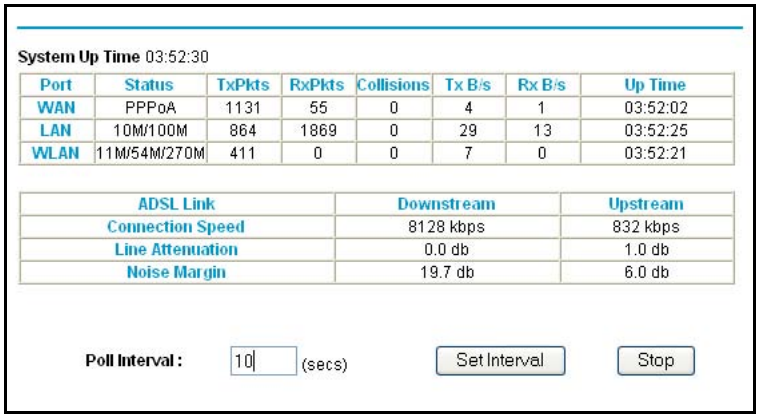
Region. The country where the unit is set up for use.

Channel. The current channel, which determines the operating frequency.

Wireless AP. Indicates if the access point feature is enabled. If disabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates if the wireless modem router is configured to broadcast its SSID.

3. Select the **Show Statistics** button on the Router Status screen to display a screen similar to this:



4. Fill in the fields as follows:

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

Status. The link status of the port.

TxPkts. The number of packets transmitted since reset or manual clear.

RxPkts. The number of packets received since reset or manual clear.

Collisions. The number of collisions since reset or manual clear.

Tx B/s. The current line utilization—percentage of current bandwidth used.

Rx B/s. The average line utilization.

Up Time. The time elapsed since the last power cycle or reset.

ADSL Link Downstream or Upstream. The statistics for the upstream and downstream DSL link. These statistics are of interest to your technical support representative if you have problems obtaining or maintaining a connection.

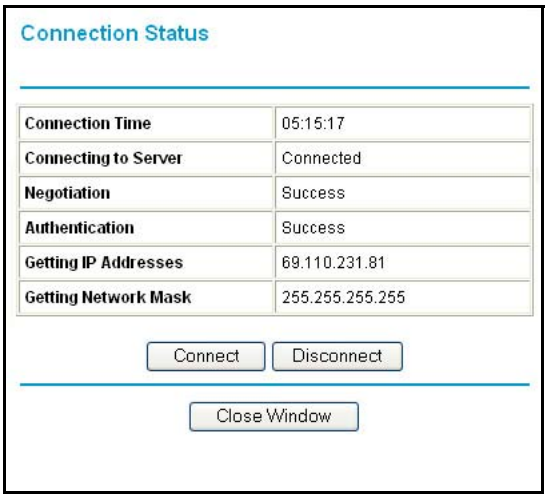
Connection Speed. Typically, the downstream speed is faster than the upstream speed.

Line Attenuation. The line attenuation increases the farther you are physically located from your ISP's facilities.

Noise Margin. The signal-to-noise ratio, which is a measure of the quality of the signal on the line.

Poll Interval. The interval at which the statistics are updated in this window. Click the **Stop** button to freeze the display.

5. In the Router Status screen, select the **Connection Status** button to display a screen similar to this:



6. Fill in the fields as follows:

Connection Time. The time elapsed since the last connection to the Internet through the DSL port.

Connecting to sender. The connection status.

Negotiation. Success or Failed.

Authentication. Success or Failed.

Obtaining IP Address. The IP address assigned to the WAN port by the ISP.

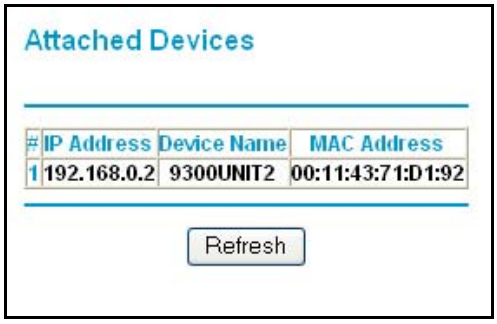
Obtaining Network Mask. The network mask assigned to the WAN port by the ISP.

View Attached Devices

The Attached Devices screen presents a table of all IP devices that the wireless modem router has discovered on the local network.

➢ **To view attached devices:**

1. Select **Maintenance > Attached Devices** to view the following table:



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

For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. Note that if the wireless modem router is rebooted, the table data is lost until the wireless modem router rediscovers the devices. To force the wireless modem router to look for attached devices, click the **Refresh** button.

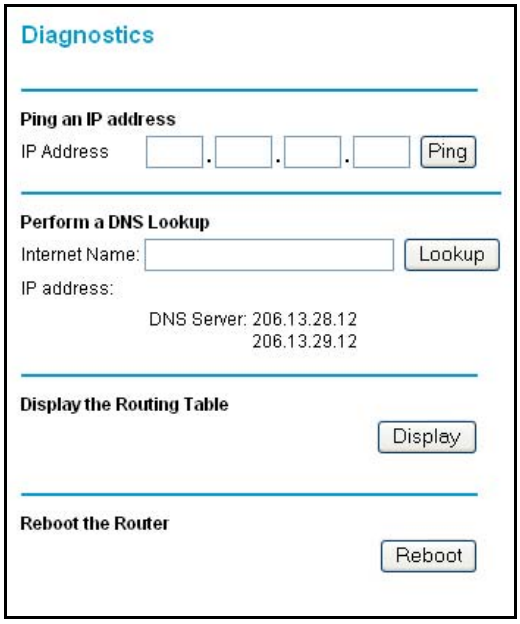
Run Diagnostic Utilities

The wireless modem router has a diagnostics feature that you can use to perform the following functions:

- Ping an IP address to test connectivity to see if you can reach a remote host.
- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing table to identify what other wireless modem routers the wireless modem router is communicating with.
- Reboot the wireless modem router to enable new network configurations to take effect or to clear problems with the wireless modem router's network connection.

➢ **To run diagnostic utilities:**

1. Select **Maintenance > Diagnostics** to display the following screen.



2. Get diagnostic information as follows:
   a. To ping an IP address, fill in the IP address and select **Ping**.
   b. To perform a DNS lookup, fill in the **Internet Name** and select **Lookup**.
   c. To display the routing table, select **Display**.
   d. Tor reboot the router, select **Reboot**.

Advanced Settings

6

Configure for unique situations

This chapter describes the advanced features of your wireless modem 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.

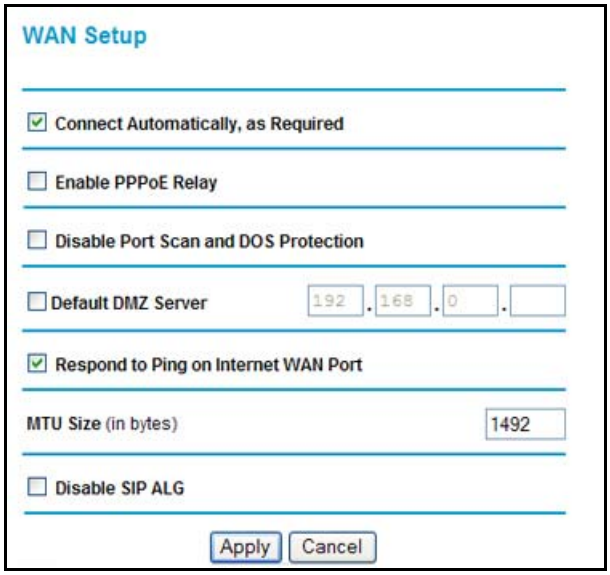
This chapter contains the following sections:

WAN Setup

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

➢ **To set up the WAN:**

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



2. Fill in the fields as follows:

Connect Automatically, as Required. This option is enabled by default so that Internet connections are made automatically whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting and connect manually from the Router Status screen. See *In the Router Status screen, select the Connection Status button to display a screen similar to this:* on page 69.

Enable PPPoE Relay. When enabled, this feature allows a PPPoE client on a local PC to connect to a remote PPPoE server with the gateway acting as a relay agent.

Disable Port Scan and DOS Protection. The firewall protects your LAN against port scans and denial of service (DOS) attacks. This protection should be disabled only in special circumstances.

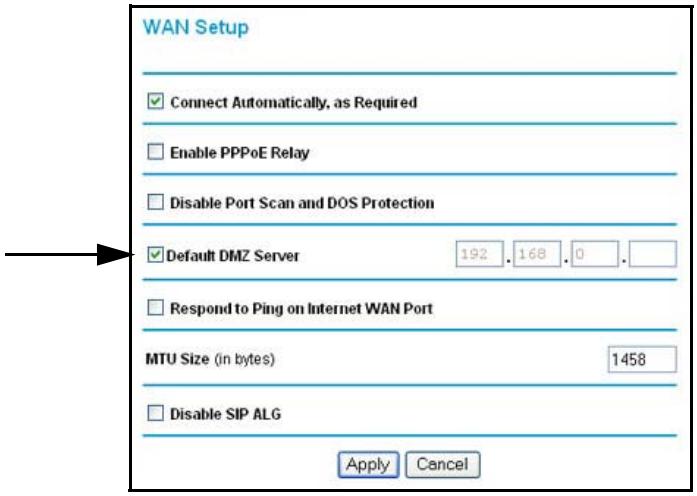
Default DMZ Server. The default demilitarized zone (DMZ) server feature is helpful when you use online games and video conferencing applications that are incompatible with NAT. The wireless modem router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

> ***Note:*** For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

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

➢ **To assign a computer or server to be a default DMZ server:**

1. In the **WAN** screen, select the **Default DMZ Server** check box.



2. Type the IP address for that server.
3. Fill in the following fields and click **Apply**:

   Respond to Ping on Internet WAN Port. If you want the wireless modem router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, because it allows your wireless modem router to be discovered. Do not select this check box unless you have a specific reason to do so.

   MTU Size (in bytes). The normal Maximum Transmit Unit (MTU) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

   Disabling the SIP ALG. The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The Disable SIP ALG check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

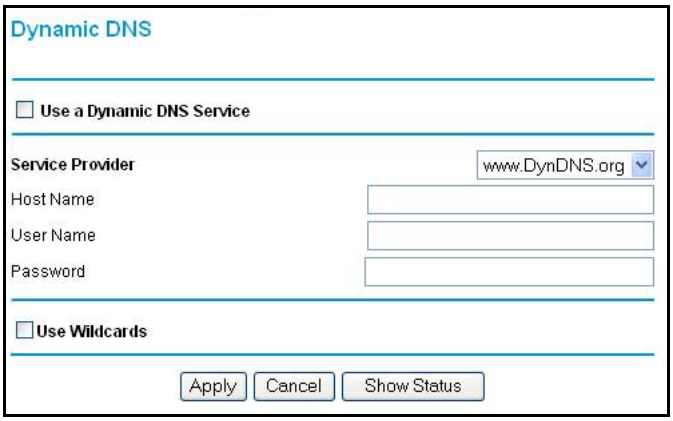
Dynamic DNS

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

The router has a client that can connect to a Dynamic DNS service provider. Once you have configured your ISP account information in the router, whenever your ISP-assigned IP address changes, your router contacts your Dynamic DNS service provider, logs in to your account, and registers your new IP address.

➢ **To set up Dynamic DNS:**

1. Select **Advanced > Dynamic DNS** to display the following screen.



2. Access the website of one of the Dynamic DNS service providers whose names appear in the **Service Provider** drop-down list, and register for an account. For example, for dyndns.org, go to www.dyndns.org.
3. Select the **Use a Dynamic DNS Service** check box.
4. Select the name of your Dynamic DNS service provider.
5. Type the host name that your Dynamic DNS service provider gave you. The Dynamic DNS service provider might call this the domain name. If your URL is myName.dyndns.org, then your host name is myName.
6. Type the user name for your Dynamic DNS account.
7. Type the password (or key) for your Dynamic DNS account.
8. 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.
9. Click **Apply** to save your settings.

Note: 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.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as DHCP and Routing Information Protocol (RIP). The wireless modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The wireless modem router's default LAN IP configuration is as follows:

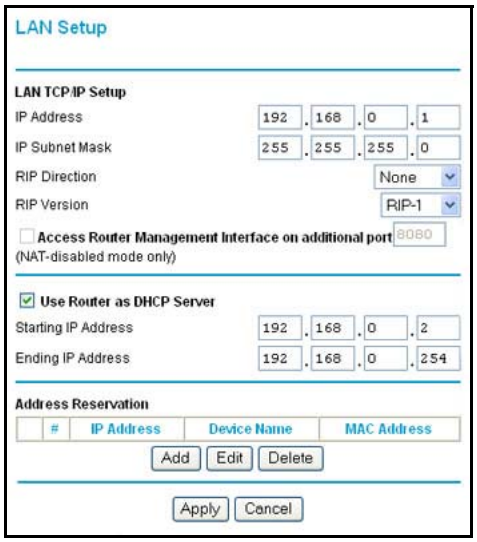
- **LAN IP address**. 192.168.0.1
- **Subnet mask**. 255.255.255.0

These addresses are part of the private address range designated by the Internet Engineering Task Force (IETF *http://www.ietf.org/*) for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in the LAN IP Setup screen.

Note: If you change the LAN IP address of the wireless modem router while connected through the browser, you are disconnected. To reconnect, open a new connection to the new IP address and log in.

➢ **To set up the LAN:**

1. Select **Advanced > LAN Setup**.



2. Enter the LAN Setup configuration and click **Apply** to save your changes.

IP Address. The LAN IP address of the wireless modem router.

IP Subnet Mask. The LAN subnet mask of the wireless modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or wireless modem router.

RIP Direction. RIP allows a wireless modem router to exchange routing information with other routers. The RIP Direction selection controls how the wireless modem router sends and receives RIP packets. The default setting is Both.

- When set to **Both** or **Out Only**, the wireless modem router broadcasts its routing table periodically.
- When set to **Both** or **In Only**, the wireless modem router incorporates the RIP information that it receives.
- When set to **None**, the wireless modem router does not send any RIP packets and ignores any RIP packets received.

RIP Version. This controls the format and the broadcasting method of the RIP packets that the wireless modem router sends. It recognizes both formats when receiving. By default, this is set for RIP-1.

- **RIP-1**. This version is universally supported. It is probably adequate for most networks, unless you have an unusual network setup.
- **RIP-2**. This version carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
- **RIP-2B**. This version uses subnet broadcasting.
- **RIP-2M**. This version uses multicasting.

Access Router Interface on Additional Port

When NAT is disabled, the wireless modem router's management interface might be accessed at the wireless modem router's LAN address using the port number you enter. This feature is not available when NAT is enabled.

Use Router as DHCP Server

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

Reserved IP Addresses Setup

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

- **To reserve an IP address:**

  1. Select **Advanced > LAN Setup** and click the **Add** button.
  2. In the **IP Address** field, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.
  3. Type the MAC address of the computer or server.

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

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

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

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

  1. Click the button next to the reserved address that you want to edit or delete.
  2. Click **Edit** or **Delete**.

Advanced Wireless Settings

➢ **To configure advanced wireless settings:**

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

Note: The advanced WPS settings section is not displayed if you selected WEP as the security option.

2. If you make changes, click **Apply**. Note that the WLAN settings come from the settings you made in the *Wireless Settings Screen* on page 37).

WLAN.

Name (SSID). The service set ID, also known as the wireless network name.

Region. The country where the unit is set up for use.

Channel. The current channel, which determines the operating frequency.

Wireless AP. Indicates if the access point feature is enabled. If disabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates if the wireless modem router is configured to broadcast its SSID.

Security. Indicates if security is configured on the wireless modem router, and if so, what type of security is configured.

WPS Settings.

Router's PIN. The PIN number that you use on a registrar (for example, from the Network Explorer on a Vista Windows PC) to configure the wireless modem router's wireless settings through WPS. You can also find the PIN on the wireless modem router's product label.

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

Keep Existing Wireless Settings. By default, the Keep Existing Wireless Settings check box is selected. This allows the modem router to keep the same SSID and wireless security settings when WPS-enabled devices are added to the network.

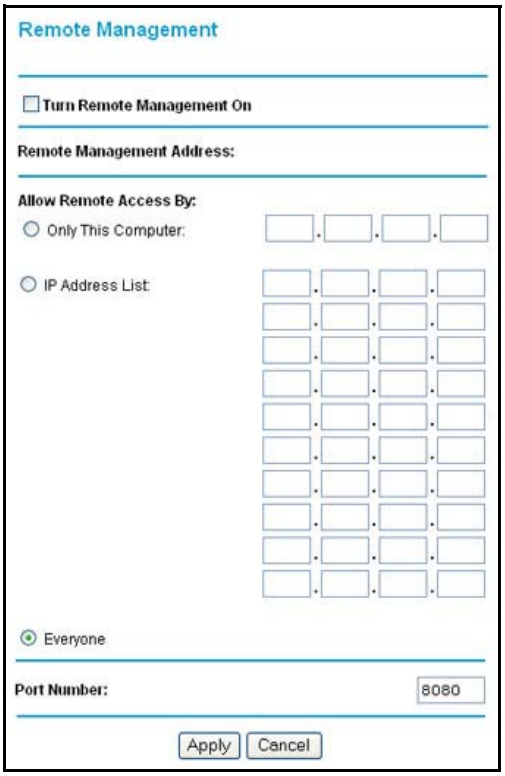
If the Keep Existing Wireless Settings check box is not selected, the next time you use WPS to connect WPS-capable devices to your wireless network, the modem router generates a new random SSID and WPA/WPA2 passphrase. NETGEAR does not recommend this.

Remote Management

The Remote Management screen lets you allow a user or users on the Internet to configure, upgrade, and check the status of your wireless modem router.

➢ **To configure remote management:**

1. Select **Advanced > Remote Management** to display this screen:



2. Select the **Turn Remote Management On** check box.
3. Specify the external addresses of wireless modem routers than can access remote management. For 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** and enter the IP address that is allowed access.
- To allow access from a range of IP addresses on the Internet, select **IP Address** and 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 to be used for accessing the router interface.

   Web browser access usually uses the standard HTTP service port 80. For greater security, you can change it so the remote router interface uses a custom port by entering that number in the field provided. 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 save your changes.

   To access your wireless modem router from the Internet, type your wireless modem router's WAN IP address in your browser's Address field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 at port number 8080, enter the following in your browser:

   http://134.177.0.123:8080

Note: The http:// is required in the address.

Static Routes

Static routes provide additional routing information to your router. Under normal 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. Only configure static routes for unusual cases such when you have multiple routers or multiple IP subnets on your network.

Static Route Example

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 192.168.0.100.
- 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 wireless modem router, and a second static route was created to your local network for all 192.168.0.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 192.168.0.100. The static route setup would look like *Figure 16, Add static routes*.

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 are to be forwarded to the ISDN router at 192.168.0.100.
- The value in the **Metric** field represents the number of routers between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.
- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

Configure Static Routes

➢ **To configure static routes:**

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

Figure 15. View additional routing information

2. To add a static route:
   a. Click **Add** to open the following screen.

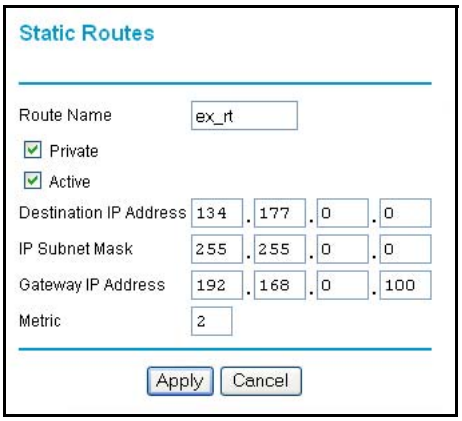


Figure 16. Add static routes

b. In the Route Name field, enter a route name for this static route. This name is for identification purpose only.

c. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.

d. Select **Active** to make this route effective.

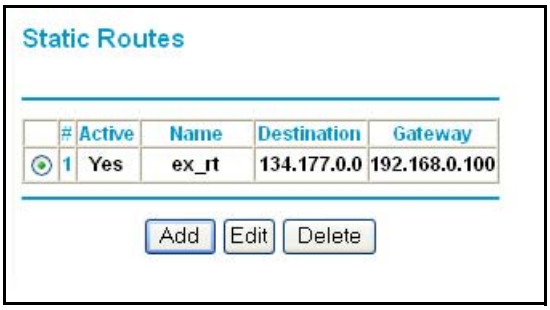
e. Enter the destination IP address of the final destination.

f. Enter the IP subnet mask for this destination. If the destination is a single host, type 255.255.255.255.

g. Enter the gateway IP address, which has to be a router on the same LAN segment as the router.

h. In the Metric field, enter a number between 2 and 15 as the metric value. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.

3. Click **Apply** to save your changes. The Static Routes table updates to show the new entry.



Universal Plug and Play

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

➢ **To configure UPnP:**

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

2. Fill in the settings as follows:

Turn UPnP On. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If UPnP is disabled, the wireless modem router

does not allow any device to automatically control the resources, such as port forwarding (mapping), of the wireless modem router.

Advertisement Period. The advertisement period is how often the wireless modem router advertises (broadcasts) its UPnP information. This value ranges from 1 to 1440 minutes. The default is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the device status freshness but can significantly reduce network traffic.

Advertisement Time To Live. This is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value is 4 hops, which works for most home networks. If you notice that some devices are not being updated or reached correctly, you might need to increase this value a little.

UPnP Portmap Table. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the wireless modem router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

3. To save, cancel your changes, or refresh the table:
   - Click **Apply** to save the new settings to the wireless modem router.
   - Click **Cancel** to disregard any unsaved changes.
   - Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Troubleshooting

7

Diagnose and solve problems

This chapter provides information to help you diagnose and solve problems you might have with your wireless modem 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:

Router Not On

When you turn the power on, the power, LAN, and DSL LEDs should light as described here. If they do not, refer to the sections that follow for help.

➢ **To check the LEDs:**

1. When power is first applied, the Power LED lights.
2. After approximately 10 seconds, the LAN and DSL LEDs light as follows:
   a. The LAN port LEDs light for any local ports that are connected.
   b. The DSL link LED lights to indicate that there is a link to the connected device.
   c. If a LAN port is connected to a 100 Mbps device, verify that the LAN port's LED is green. Note that if the LAN port is 10 Mbps, the LED is amber.

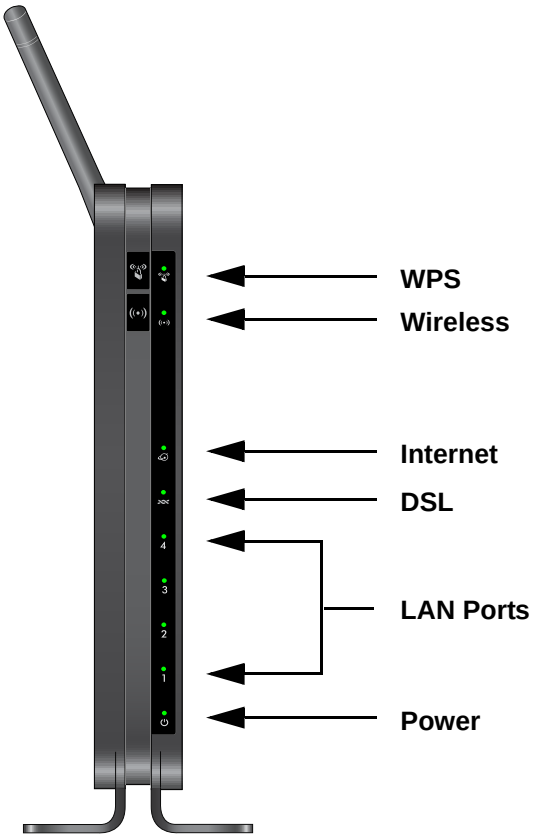


Figure 17. Front panel LED Icons

Power LED Is Off

If the Power and other LEDs are off when your router is turned on:

- Check that the power cord is correctly connected to your router and the power supply adapter is correctly connected to a functioning power outlet.

- Check that you are using the 12-V DC power adapter supplied by NETGEAR for this product.

If the error persists, you could have a hardware problem and should contact NETGEAR Technical Support.

Power LED Is Red

When the router is turned on, it performs a power-on self-test. If the Power LED turns red after a few seconds or at any other time during normal operation, there is a fault within the router.

If the Power LED turns red to indicate a router fault, turn the power off and on to see if the wireless modem router recovers. If the power LED is still red 1 minute after power-up:

- Turn the power off and on one more time to see if the wireless modem router recovers.
- Clear the router's configuration to factory defaults as explained in *Factory Settings* on page 94. This sets the router's IP address to 192.168.0.1.

If the error persists, you could have a hardware problem and should contact NETGEAR Technical Support.

LAN or DSL Link LED Is Off

If either the LAN or DSL link LED does not light when the Ethernet connection is made, check the following:

- The Ethernet cable connections are secure at the router and at the hub or workstation.
- The power is turned on to the connected hub or workstation.
- You are using the correct cable. When connecting the DSL port, use the cable that was supplied with the wireless modem router. If the DSL link LED is still off, this could mean that there is no DSL service or the cable connected to the DSL port is bad.

See also *DSL Link LED Is Off* on page 88.

No Internet Connection

If your router cannot access the Internet, first check the DSL connection, and then check the WAN TCP/IP connections. See *Figure 17, Front panel LED Icons* on page 86 for the location of the LEDs.

DSL Link

First determine whether you have a DSL link with the service provider. The state of this connection is indicated by the DSL LED.

DSL Link LED Is Green or Blinking Green

You have a good DSL connection. The service provider has connected your line correctly, and your wiring is correct.

DSL Link LED Is Blinking Amber

Your wireless modem router is attempting to make a DSL connection with the service provider. The LED should turn green within several minutes.

If the DSL link LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and use a microfilter on each telephone as described in *ADSL Microfilters* on page 13. If you connect the microfilters correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL link LED, there might be a problem with your wiring. If the telephone company has tested the DSL signal at your network interface device (NID), you might have poor-quality wiring in your house.

DSL Link LED Is Off

First disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL link LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the DSL service. It could be necessary to use a swapper if your DSL signal is on pins 1 and 4 or the RJ-11 jack. The wireless modem router uses pins 2 and 3.

Internet LED Is Red

If the Internet LED is red, the device could not connect to the Internet. Verify the following:

- Check that your log-in credentials are correct. See *Log In to the N150 Modem Router* on page 21 for more information.
- Check that the information you entered on the Basic Settings screen is correct. See *Manual Setup (Basic Settings)* on page 25.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the DSL settings screen are correct.
- Find out if the ISP is having a problem. If it is, wait until that problem is cleared up and try again.

Cannot Obtain an Internet IP Address

If your wireless modem router cannot access the Internet, and your Internet LED is green or blinking green, check whether the wireless modem router can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your wireless modem router has to request an IP address from the ISP. You can determine whether the request was successful as follows:

1. Access the router menus at **http://192.168.0.1** and log in.
2. Under Maintenance, select **Router Status** and check that an IP address shows for the WAN port. If 0.0.0.0 shows, your wireless modem router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrect. See *Debug PPPoE or PPPoA* on page 89.
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account to the wireless modem router in the browser-based Setup Wizard. See *Setup Wizard* on page 24 for more information.
- Your ISP allows only one Ethernet MAC address to connect to the 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 spoof your computer's MAC address through the Basic Settings screen. See *Manual Setup (Basic Settings)* on page 25.

Debug PPPoE or PPPoA

➢ **To debug the PPPoE or PPPoA connection:**

1. Access the router menus at **http://192.168.0.1** and log in.
2. Under Maintenance, select **Router Status**.
3. Click the **Connection Status** button.
4. If all of the steps indicate OK, your PPPoE or PPPoA connection is working.
5. If any of the steps indicate Failed, you can attempt to reconnect by clicking **Connect**.

   The wireless modem router continues to attempt to connect indefinitely. If you do not connect after several minutes, check that the service name, user name, and password you are using are correct. Also check with your ISP to be sure that there is no problem with their service.

> ***Note:*** Unless you connect manually, the wireless modem router does not authenticate with PPPoE or PPPoA until data is transmitted to the network.

Cannot Load an Internet Web Page

If your wireless modem router can obtain an IP address, but your browser cannot load any Internet web pages:

- 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 wireless modem router's configuration, reboot your computer, and verify the DNS address. Alternately, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

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

TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers have a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

Test the LAN Path to Your Wireless Modem Router

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

➢ **To ping the router from a PC running Windows 95 or later:**

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

   ping 192.168.0.1

3. Click **OK**.
   a. You should see a message like this one:

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

b. If the path is working, you see this message:

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

c. 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
  - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in *LAN or DSL Link LED Is Off* on page 87.
  - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After you verify that the LAN path works correctly, test the path from your PC to a remote device. In the Windows Run screen, 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 as described in *Test the LAN Path to Your Wireless Modem Router* on page 90 display. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default wireless modem router. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default wireless modem router.
- Check that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single PC connected to that modem. In this case, configure your router to clone or spoof the MAC address from the authorized PC.

Cannot Log in

If you cannot log in to the wireless modem router from a computer on your local network, check the following:

- The router is plugged in and it is on.
- You are using the correct login information. The login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.
- If you cannot connect wirelessly, try an Ethernet connection and view the router wireless settings and set up your wireless computer with corresponding wireless settings.
- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router. The LAN LED for the port you are using on the router should light up to show your connection.
- 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 192.168.0.2 to 192.168.0.254.
- If the computer IP address is 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address when the computer cannot reach a DHCP server. The auto-generated addresses are in the range 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 as explained in *Factory Settings* on page 94. This sets the router's IP address to 192.168.0.1.
- 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 closing the browser and relaunching it.

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.

Firmware Needs to Be Reloaded

When you attempt to connect to the Internet, the browser might display a message similar to the one below telling you that you need to reload the router's firmware. This means a problem has been detected with the router's firmware.

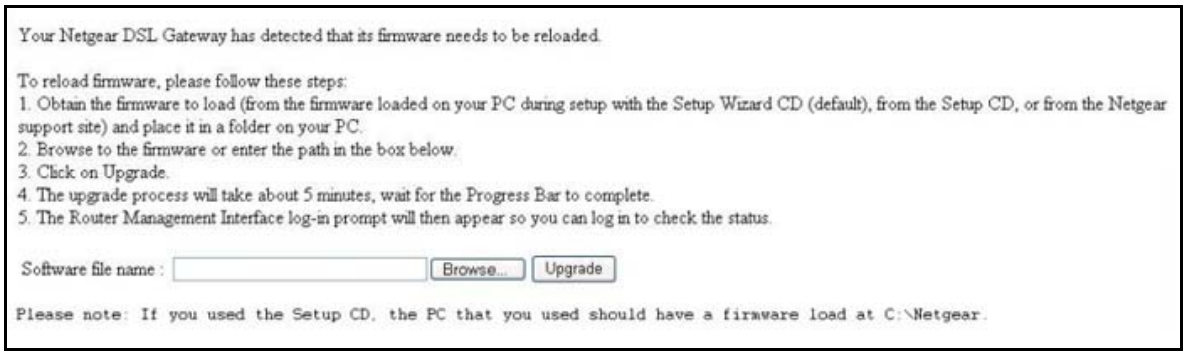


Figure 18. Reload firmware

➢ **To reload the firmware:**

1. If you already have the firmware file on your PC, go directly to *step 2*. If you do not have the firmware file on your PC, obtain the firmware from the NETGEAR support site at *http://support.netgear.com*through another working Internet connection.
2. Click **Browse**.
3. Navigate to the firmware file.
4. Click **Upgrade**. A progress bar displays. The reload takes about 5 minutes to complete. When the firmware recovery is completed, the login screen displays so you can log in.

Incorrect Date or Time

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

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

Technical Specifications

A

This appendix includes the factory default settings, technical specifications for the N150 Wireless ADSL2+ Modem Router DGN1000, related documents, and instructions for wall-mounting the unit.

This appendix contains the following sections:

Factory Settings

You can return the wireless modem router to its factory settings. On the bottom of the wireless modem router, use the end of a paper clip or some other similar object to press and hold the Restore Factory Settings button for at least 7 seconds. The wireless modem router resets, and returns to the factory settings. Your device will return to the factory configuration settings shown in the following table.

Feature		Default Behavior
Router Login		
	User Login URL	http://www.routerlogin.net *or* http://www.routerlogin.com
	User Name (case-sensitive)	admin
	Login Password (case-sensitive)	password
Internet Connection		
	WAN MAC Address	Use default address
	WAN MTU Size	1492
	Port Speed	AutoSense

Feature		Default Behavior
Local Network (LAN)		
	Lan IP	192.168.0.1
	Subnet Mask	255.255.255.0
	RIP Direction	None
	RIP Version	Disabled
	RIP Authentication	None
	DHCP Server	Enabled
	DHCP Starting IP Address	192.168.0.2
	DHCP Ending IP Address	192.168.0.254
	DMZ	Disabled
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving 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

Feature		Default Behavior
Wireless		
	Wireless Communication	Enabled
	Wi-Fi Network Name (SSID)	Can be found on the router label at the bottom of the unit
	WPA/WPA2-PSK Passphrase	Can be found on the router label at the bottom of the unit
	Broadcast SSID	Enabled
	Transmission Speed	Auto[1]
	Country/Region	United States (in North America; otherwise, varies by region)
	RF Channel	Auto
	Operating Mode	Up to 150 Mbps
	Data Rate	Best
	Output Power	Full
	Access Point	Enabled
	Authentication Type	Pre-Shared Key
	Wireless Card Access List	All wireless stations allowed

1. 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

Network Protocol and Standards Compatibility		
Data and routing protocols:		TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power Adapter		
	North America	120V, 60 Hz, input
	UK, Australia	240V, 50 Hz, input
	Europe:	230V, 50 Hz, input
	All regions (output)	12 V AC @ 1.0A output
Physical		
	Dimensions	6.80 in. x 5.03 in. x 1.28 in. 172.7 mm x 127.7 mm x 32.5 mm
	Weight	0.61 lbs. 0.275 kg
Environmental		
	Operating temperature	0° to 40° C (32º to 104º F)
	Operating humidity	10% to 90% relative humidity, noncondensing
	Storage temperature	-20° to 70° C (-4º to 158º F)
	Storage humidity	5 to 95% relative humidity, noncondensing
Regulatory Compliance		
	Meets requirements of	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Interface Specifications		
	LAN	10BASE-T or 100BASE-Tx, RJ-45
	WAN	DSL, Dual RJ-11, pins 2 and 3 T1.413, G.DMT

Notification of Compliance

B

NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

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

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

Europe – EU Declaration of Conformity

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 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 N150 Wireless ADSL2+ Modem Router DGN1000 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

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

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

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N150 Wireless ADSL2+ Modem Router DGN1000) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

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

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

Industry Canada

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

IMPORTANT NOTE: Radiation Exposure Statement:

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

Caution:

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

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

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

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

E

F

G

H

I

K

L

M

T

U

V

W