NETGEAR®

Wireless-N 150 Router
WNR612v2

User Manual

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

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

Phone (Other Countries): See Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

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.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10614-01	v1.0	July 2010	

Table of Contents

Chapter 7   Troubleshooting

Appendix A   Factory Default Settings and Technical Specifications

Appendix B   Related Documents

Appendix C   Notification of Compliance

Index

Configuring Your Internet Connection

1

> **Note:** For help with installation and initial setup, see the *Wireless-N 150 Router WNR612v2 Installation Guide* included in the package.

This chapter describes how to configure your Wireless-N 150 Router WNR612v2 Internet connection. This chapter includes:

- *Logging In to Your Wireless Router* on page 7
- *Selecting a Language for Your Screen Display* on page 8
- *Using the Setup Wizard* on page 9
- *Viewing or Manually Configuring Your ISP Settings* on page 9

Logging In to Your Wireless Router

You can log in to the wireless router to view or change its settings, and to access the Knowledge Base and documentation.

To log in to the wireless router:

1. If you have not set up wireless connections yet, connect your computer to the wireless router with an Ethernet cable.

2. In the address field of your Internet browser, enter **http://www.routerlogin.com**. or **http://www.routerlogin.net**.

   To connect, you can also enter the router's IP address, **http://192.168.1.1**.

   The wireless router user name and password are not the same as any other user name or password you might use to log in to your Internet connection.

3. Enter **admin** for the user name and your password (or the default, **password**).

   For information about how to change the password, see *Changing the Administrator Password* on page 27.

4. The screen that displays when you log in depends on whether the wireless router has already been set up.

   - **Firmware Upgrade Assistant**: If you log in after the wireless router has been configured, this screen displays. See *Upgrading the Firmware* on page 44for details.

   - **Router Status screen**: The wireless router Internet connection is not configured, or the wireless router has been reset to its factory default settings. See *Viewing Wireless Router Status Information* on page 47.

   - **Basic Settings screen**: If there is no new firmware and your Internet connection is configured, the Basic Settings screen displays. See *Viewing or Manually Configuring Your ISP Settings* on page 9.

   If you do not click **Logout**, the wireless router will wait for 5 minutes after no activity before it automatically logs you out.

Selecting a Language for Your Screen Display

Using the Select Language drop-down list, located in the upper right corner of the Router Manager screen, you can change the language.
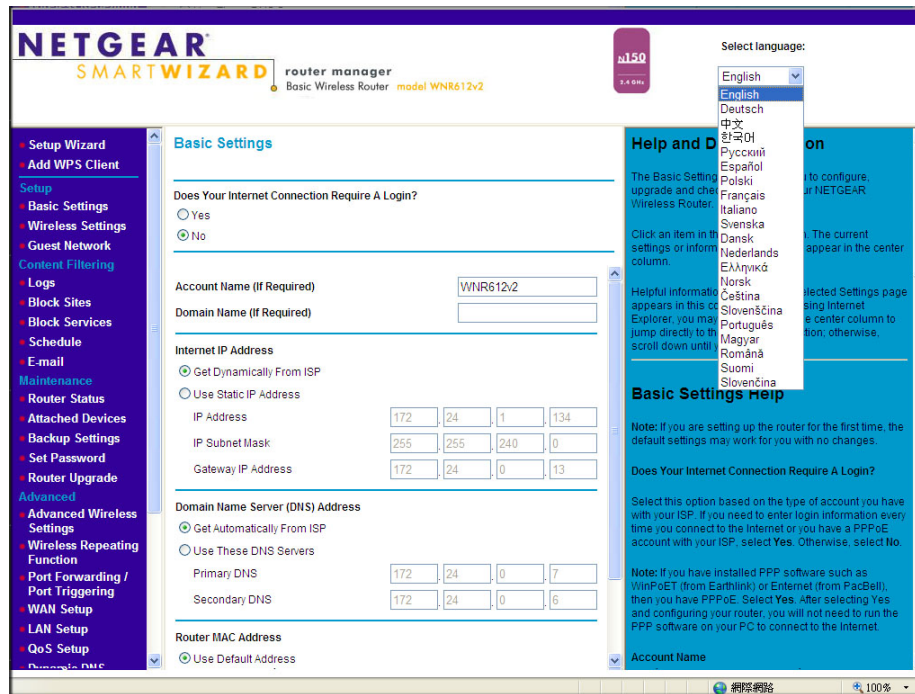
The language is set to English by default. The default language is always stored in memory. When you select another language, it is stored in memory in addition to English. The additional language stored is the most recently selected. For example, if you select Deutsch, German and English will be stored. If you next select Chinese, Chinese and English will be stored.

To change the displayed language:

1. Expand the list and select the language you want.
2. Click **Apply**.

    The language you select is then downloaded and displayed in the language selection box, and your screen display will be in the selected language.

> **Note:** You can select from the entire list of supported languages only when the router is connected to the Internet. When the router is not connected to the Internet, you can select only one of the stored languages.

Using the Setup Wizard

The Setup Wizard can check your Internet connection for servers and protocols to determine your ISP configuration. This feature is not the same as the Smart Wizard on the *Resource CD* that is used for installation. You can also manually specify your Internet connection settings in the Basic Settings screen.

To use the Setup Wizard:

1. From the top of the router main menu, select Setup Wizard.
2. Make sure the correct location is in the **Country** field.
3. Select the **Yes** radio button to use the wizard, and click **Next** to proceed.
4. Depending on the type of connection, you are prompted to enter your ISP settings.
5. At the end of the Setup Wizard, click **Test** to check your Internet connection. If you have trouble connecting to the Internet, see Chapter 7, *Troubleshooting*.

Viewing or Manually Configuring Your ISP Settings

To view or configure the basic settings:

1. Select Basic Settings from the router menu.
2. Select **Yes** or **No** depending on whether your ISP requires a login. This selection changes the fields available on the Basic Settings screen.

- **Yes**. If your ISP requires a login, select this radio button.
- **No**. Enter the account name, if required, and the domain name, if required.

3. Enter the settings for the IP address and DNS server. If you enter or change a DNS address, restart the computers on your network so that these settings take effect.

4. If no login is required, you can specify the MAC Address setting.

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

6. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within 1 minute, see *Checking the Internet Service Connection* on page 75.

When your Internet connection is working, you do not need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your wireless router automatically logs you in.

Table 1. Basic Settings Screen Fields

Settings		Description
Does Your ISP Require a Login?		• Yes • No
These fields appear only if no login is required.	Account Name (If required)	Enter the account name provided by your ISP. This might also be called the host name.
	Domain Name (If required)	Enter the domain name provided by your ISP.
These fields appear only if your ISP requires a login.	Internet Service Provider	PPPoE, PPTP, or L2TP
	Login	The login name provided by your ISP. This is often an e-mail address.
	Password	The password that you use to log in to your ISP.
	Service Name	If your ISP provided a service name, enter it here.
	Connection Mode	Select the connection mode: Always on, Dial on Demand, or Manually Connect.
	Idle Timeout (In minutes)	If you want to change the Internet login time-out, enter a new value in minutes. This determines how long the wireless router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out.
Internet IP Address		• **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses. • **Use Static IP Address**. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP's wireless router to which your wireless router will connect.
Domain Name Server (DNS) Address		The DNS server is used to look up site addresses based on their names. • **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS server address automatically. • **Use These DNS Servers**. If you know your ISP does not automatically transmit DNS addresses to the wireless 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.

Table 1. Basic Settings Screen Fields (Continued)

Settings		Description
This field appears only if your ISP does not require a login.	Router MAC Address	Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address. • **Use Default MAC Address**. This is the usual setting. • **Use Computer MAC address.** If your ISP requires MAC authentication, you can use this setting to disguise the wireless router's MAC address with the computer's own MAC address. • **Use This MAC Address**. If your ISP requires MAC authentication, you can manually type the MAC address for a different computer. The format for the MAC address is XX:XX:XX:XX:XX:XX.

Wireless Configuration

2

This chapter describes how to configure your wireless connection. This chapter includes:

For a wireless connection, the SSID, also called the wireless network name, and the wireless security settings must be the same for the wireless router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.

> **Note:** Computers can connect wirelessly at a range of several hundred feet. If you do not use wireless security, this can allow others outside your immediate area to access your network.

Planning Your Wireless Network

For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.

- To manually configure the wireless settings, you must know the following:
    - SSID. The default SSID for the wireless router is NETGEAR.
    - The wireless mode (80.211n, 802.11g, or 802.11b) that each wireless adapter supports.
    - Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

    See *Manually Configuring Your Wireless Settings* on page 14.

- Push 'N' Connect (WPS) implements WPA/WPA2 wireless security on the wireless router and your wireless computer or device at the same time. The wireless computer or device must be compatible with WPS.

    See *Using Push 'N' Connect (WPS) to Configure Your Wireless Network* on page 18.

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the wireless router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

For best results, place your wireless router according to the following guidelines:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.
- If using 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).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Wireless Security Options

Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The Wireless-N 150 Router WNR612v2 provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

There are several ways you can enhance the security of your wireless network:

*   **Turn off the broadcast of the wireless network name (SSID)**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network discovery feature of some products, such as Windows XP, but the data is still exposed.

*   **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.

*   **WPA-PSK (TKIP), WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise.

For more information about wireless technology, click the link to the online document in Wireless Networking Basics in Appendix B.

Manually Configuring Your Wireless Settings

> **Note:** If you use a wireless computer to change the wireless network name (SSID) or wireless security, you will be disconnected when you click **Apply**. To avoid this problem, connect your computer to the router with an Ethernet cable while you are making changes.

To view or manually configure the wireless settings:

1. Log in to the wireless router as described in *Logging In to Your Wireless Router* on page 7.

2. Select Wireless Settings from the main menu:

The settings for this screen are explained in Table 2.

3. Select the region in which the wireless router will operate.

4. For initial configuration and test, leave the other settings unchanged.

5. To save your changes, click **Apply**.

6. Configure and test your computers for wireless connectivity.

   Set up your wireless computers with the same SSID and wireless security settings as your wireless router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the wireless router. If there is interference, adjust the channel.

Table 2. Wireless Settings

Settings		Description
Region		The location where the wireless router is used.
Wireless Network	Enable SSID Broadcast	If this check box is selected, the SSID is broadcast in the selected channel.
	Enable Wireless Isolation	If this check box is selected, computers will not be able to connect wirelessly to the wireless router.
	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. When there is more than one wireless network, SSIDs provide a means for separating the traffic. To join a network, a wireless computer or device must use the SSID.

Table 2. Wireless Settings (Continued)

Settings		Description
Wireless Network (Continued)	Channel	The wireless channel: 1 through 13. This setting applies to any guest networks you set up. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to try different channels to see which is best. The number of available channels varies by region and depends on the selected mode.
	Mode The mode can be set only for the primary wireless LAN (NETGEAR).	• **Up to 150 Mbps** (default setting): Allows wireless stations that support speeds up to 150 Mbps. The router transmits two streams with different data concurrently on the same channel. This mode restricts channel bandwidth to minimize interference with the transmissions of other wireless networks. • **Up to 65 Mbps**: Neighbor Friendly Mode - Will not interfere with neighboring wireless networks. • **Up to 54 Mbps**: Allows wireless stations that support speeds up to 54 Mbps.
Security Options	None	You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security.
	WEP	Use encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. See *Configuring WEP* on page 16.
	WPA-PSK (TKIP)	Allow only computers configured with WPA to connect to the wireless router. See the following section, *Configuring WEP* on page 16.
	WPA2-PSK (AES)	Allow only computers configured with WPA2 to connect to the wireless router. See *Configuring WPA, WPA2, or WPA + WPA2* on page 18.
	WPA-PSK (TKIP) + WPA2-PSK (AES)	Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless router. See *Configuring WPA, WPA2, or WPA + WPA2* on page 18.

Configuring WEP

WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools.

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click **Apply**. Reconfigure your wireless computer to match the new settings, or access the wireless router from a wired computer to make further changes.

To configure WEP data encryption:

1. Log in to the wireless router as described in *Logging In to Your Wireless Router* on page 7.

2. From the main menu, select Wireless Settings to display the Wireless Settings screen.

3. In the Security Options section, select the **WEP** radio button:

4. Select the **Authentication Type**: **Automatic**, or **Shared Key**. The default is Automatic.

> **Note:** *The authentication is separate from the data encryption. You can select authentication that requires a shared key, but still leaves data transmissions unencrypted. Security is stronger if you use both the Shared Key and WEP encryption settings.*

5. Select the **Encryption Strength** setting:

   • **WEP 64-bit encryption**. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).

   • **WEP 128-bit encryption**. Enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).

6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network:

   • **Passphrase**. To use a passphrase to generate the keys, enter a passphrase, and click **Generate**. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the wireless router.

> **Note:** Not all wireless adapters support passphrase key generation.

   • **Key 1**–**Key4**. These values are *not* case-sensitive. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).

7. Select which of the four keys will be the default.

   Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected.

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

Configuring WPA, WPA2, or WPA + WPA2

Both WPA and WPA2 provide strong data security. WPA with TKIP is a software implementation that can be used on Windows systems with Service Pack 2 or later, WPA2 with AES is a hardware implementation; see your device documentation before implementing it. Consult the product documentation for your wireless adapter for instructions for configuring WPA settings.

> **Note:** If you use a wireless computer to configure wireless security settings, you will be disconnected when you click **Apply**. If this happens, reconfigure your wireless computer to match the new settings, or access the wireless router from a wired computer to make further changes.

To configure WPA or WPA2 in the wireless router:

1. Log in to the wireless router as described in *Logging In to Your Wireless Router* on page 7.
2. Select Wireless Settings from the main menu.
3. On the Wireless Setting screen, select the radio button for the WPA or WPA2 option of your choice.
4. The settings displayed on the screen depend on which security option you select.
5. For WPA-PSK or WPA2-PSK, enter the passphrase.
6. To save your settings, click **Apply**.

Using Push 'N' Connect (WPS) to Configure Your Wireless Network

For you to use Push 'N' Connect, your wireless computers or devices must support Wi-Fi Protected Setup (WPS). Compatible equipment usually has the WPS symbol on it. WPS can configure the network name (SSID) and set up WPA/WPA2 wireless security for the wireless router and the wireless computer or device at the same time.

Some considerations regarding WPS are:

- NETGEAR's Push 'N' Connect feature is based on the WPS standard. All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.

- If your wireless network will include a combination of WPS-capable devices and non-WPS-capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding WPS-capable devices.

You can connect to the network using WPS either with a push button or a PIN.

- **Push Button**. This is the preferred method. See the following section, WPS Button.
- **Entering a PIN**. See *WPS PIN Entry* on page 20.

WPS Button

Any wireless computer or wireless adapter that will connect to the wireless router wirelessly is a client. The client must support a WPS button, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

To use the wireless router WPS button to add a WPS client:

1. Log in to the wireless router as described in *Logging In to Your Wireless Router* on page 7.

2. On the wireless router main menu, select Add a WPS Client, and then click **Next**.

   By default, the **Push Button (recommended)** radio button is selected.

   Add WPS Client

   Select a setup method:
   ⊙ Push Button (recommended)
   You can either press the Push Button physically on the router or press the Button below (soft Push Button)

   ○ PIN Number

   WPS button

3. Either click the onscreen button or press the WPS button on the front of the wireless router.

   The wireless router tries to communicate with the client (the computer that wants to join the network) for 2 minutes.

4. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button.

5. Go back to the wireless router screen to check for a message.

   The wireless router WPS screen displays a message confirming that the client was added to the wireless network. The wireless router generates an SSID, and implements WPA/WPA2 wireless security. The wireless router keeps these wireless settings unless you change them, or

   WPS Settings

   WPS Settings
   Router's PIN: 12345670
   ☑ Keep Existing Wireless Settings

   [Apply] [Cancel]

   you clear the **Keep Existing Wireless Settings** check box in the WPS Settings screen.
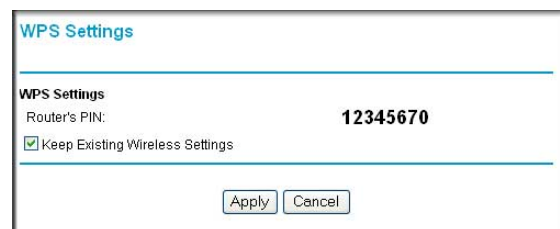
6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See *Manually Configuring Your Wireless Settings* on page 14.

To access the Internet from any computer connected to your wireless router, launch an Internet browser such as Mozilla Firefox. You should see the wireless router's Internet LED blink, indicating communication to the ISP.

> **Note:** If no WPS-capable client devices connect during the 2-minute time
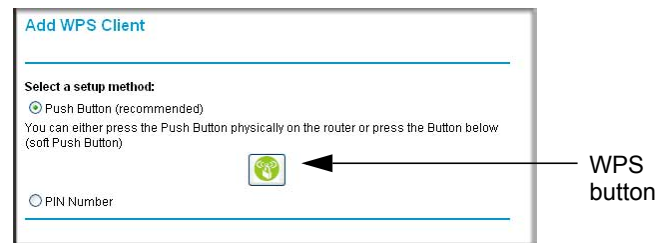> frame, the wireless settings do not change on the wireless router.

WPS PIN Entry

Any wireless computer or device that will connect to the wireless router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

The first time you add a WPS client, make sure that the **Keep Existing Wireless Settings** check box on the WPS Settings screen is cleared. This is the default setting for the wireless router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the wireless router automatically selects this check box so that your SSID and wireless security settings stay the same if other WPS devices are added later.

To use a PIN to add a WPS client:

1. Log in to the wireless router as described in *Logging In to Your Wireless Router* on page 7.

2. On the wireless router main menu, select Add a WPS Client (computers that will connect wirelessly to the wireless router are clients), and then click **Next**. The Add WPS Client screen displays:

3. Select the **PIN Number** radio button.

4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN. Take note of the client PIN.

5. From the wireless router Add WPS Client screen, enter the client PIN number, and click **Next**.

   • The wireless router tries to communicate with the client for 4 minutes.

   • The wireless router WPS screen confirms that the client was added to the wireless network. The wireless router generates an SSID, and implements WPA/WPA2 wireless security.

   • If the client is not added during the 2-minute time frame, the router wireless settings remain unchanged.

6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See *Manually Configuring Your Wireless Settings* on page 14.

To access the Internet from any computer connected to your wireless router, launch an Internet browser. You should see the wireless router's Internet LED blink, indicating communication to the ISP.

Adding Wireless Computers That Do Not Support WPS

If you set up your network with WPS, and now you want to add a computer that does not support WPS, you must manually configure that computer. For information about how to view the wireless settings for the router, see *Manually Configuring Your Wireless Settings* on page 14.

Because WPA randomly creates the SSID and WPA/WPA2 keys, they might be difficult to type or remember (that is one reason why the network is so secure). You can change the wireless settings so that they are easier for you to remember. If you do that, then you will need to set up the WPS-compatible computers again.

Changing wireless settings for the network:

> **Note:** Making these changes will cause all wireless computers to be disconnected from network. You will then have to set them up with the new wireless settings.

---

1. Use an Ethernet cable to connect a computer to the router. That way you will not get disconnected when you change the wireless settings.

2. Log in to the router and select Wireless Settings (see *Manually Configuring Your Wireless Settings* on page 14).

3. Make the following changes:
   - Change the wireless network name (SSID) to a meaningful name.
   - On the WPA/PSK + WPA2/PSK screen, select a passphrase.
   - Make sure that the **Keep Wireless Settings** check box is selected in the WPS Settings screen so that your new settings will not be erased if you use WPS.

4. Click **Apply** so that your changes take effect. Write down your settings.

   All wireless clients are disassociated and disconnected from the wireless router.

5. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the security settings that you selected in Step 3 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).

6. For the WPS devices that you want to connect, follow the procedure in *WPS Button* on page 19 or *WPS PIN Entry* on page 20.

   The settings that you configured in Step 3 are broadcast to the WPS devices so that they can connect to the wireless router.

Wireless Guest Networks

A wireless guest network allows you to provide guests access to your wireless network without prior authorization of each individual guest. You can configure wireless guest networks and specify the security options for each wireless guest network.

To configure a wireless guest network:

1. In the main menu, under Setup, select Wireless Settings.

2. Select any of the following Wireless settings:

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

    • **Enable SSID Broadcast** – If selected, the Wireless Access Point broadcasts its name (SSID) to all Wireless Stations. Stations can adopt the correct SSID for connections to this Access Point.

    • **Allow Guest to access MY Local Network** – If selected any user who connects to this SSID can access local networks associated with the router like users in the primary SSID.

3. Give the wireless network a name.

    The name is case-sensitive and can be up to 32 characters. The same name must be assigned to all wireless devices in your network. NETGEAR recommends that you change the name to a different value.

4. Select a Security option from the list.

5. Click **Apply** to save your selections.

Advanced Wireless Settings

This section describes the wireless settings that you can view and specify in the Advanced Wireless Settings screen, which you access under Advanced in the main menu.

To configure the advanced wireless security settings:

1. Log in to the router as described in *Logging In to Your Wireless Router* on page 7.

2. Select Wireless Settings under Advanced in the main menu. The advanced Wireless Settings screen displays:

The available settings in this screen are:

- **Enable Wireless Router Radio**. If you disable the wireless router radio, wireless devices cannot connect to the wireless router. If you will not be using your wireless network for a period of time, you can clear this check box and disable all wireless connectivity.

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

- **Transmit Power Control.** There are four different settings for transmit power control: 100% (the default), 75%, 50%, and 25%.

- **WPS Settings**. For information about these settings, see *Using Push 'N' Connect (WPS) to Configure Your Wireless Network* on page 18.

- **Wireless Card Access List**. For information about this list, see *Restricting Wireless Access by MAC Address* on page 24.

Advanced WPS Settings

On the Advanced Wireless Setting screen, these WPS Settings are available:

- **Router's PIN**. The PIN is displayed so that you can use it to configure the router through WPS (Wi-Fi Protected Setup). It is also displayed on the router's label.

- **Disable Router's PIN**. If the router's PIN is disabled, you cannot configure the router's wireless settings with WPS. However, if your settings are already configured, you can still add WPS-enabled wireless clients. The router might disable the PIN if it detects suspicious attempts to break into your wireless settings; this can happen if the

check box is selected. You can enable the PIN by clearing the check box and clicking **Apply**.

- **Keep Existing Wireless Settings**. This check box is automatically selected after WPS is enabled to prevent unwanted settings changes, and is also selected if you have already specified wireless security settings or your SSID without using WPS. When this check box is *not* selected, adding a new wireless client using the Add WPS Client screen (see *Using Push 'N' Connect (WPS) to Configure Your Wireless Network* on page 18) changes the router's SSID and security passphrase. You might need to clear it if you are using certain registrars, such as for a Windows Vista PC, to configure the router through WPS.

Restricting Wireless Access by MAC Address

When a Wireless Card Access List is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computers list.

The Wireless Card Access List displays a list of wireless computers that you allow to connect to the router based on their MAC addresses. These wireless computers must also have the correct SSID and wireless security settings to access the wireless router.

The MAC address is a network device's unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). It can usually be found on the bottom of the wireless card or network interface device. If you do not have access to the physical label, you can display the MAC address using the network configuration utilities of the computer. In WindowsXP, for example, typing the `ipconfig/all` command in an MSDOS command prompt window displays the MAC address as Physical Address. You might also find the MAC addresses in the router's Attached Devices screen.

To restrict access based on MAC addresses:

1. Select Wireless Settings under Advanced in the main menu.

2. In the Advanced Wireless Settings screen, click **Setup Access List** to display the Wireless Card Access List.
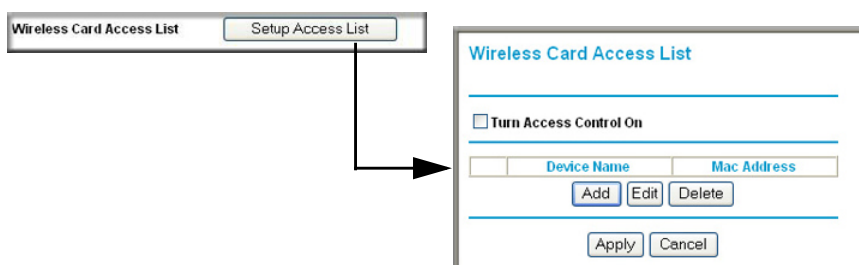
3. Click **Add** to add a wireless device to the wireless access control list. The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

Wireless Card Access Setup

Available Wireless Cards

	Device Name	MAC Address
⊙	9300UNIT2	00:0f:b5:0d:ab:19

Wireless Card Entry

Device Name: 9300UNIT2

MAC Address: 00:0f:b5:0d:ab:19

[Add] [Cancel] [Refresh]

4. If the computer you want appears in the Available Wireless Cards list, you can select the radio button of that computer to capture its MAC address; otherwise, you can manually enter a name and the MAC address of the authorized computer. You can usually find the MAC address on the bottom of the wireless device.

> **Tip:** You can copy and paste the MAC addresses from the router's Attached Devices screen into the MAC Address field of this screen. To do this, configure each wireless computer to obtain a wireless link to the router. The computer should then appear in the Attached Devices screen.

5. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.

6. Repeat step 3 through step 5 for each additional device you want to add to the list.

7. Select the **Turn Access Control On** check box.

> **Note:** If you connected wirelessly to the router, make sure your computer is on the access control list before you select **Turn Access Control On**, and click **Apply**. Otherwise, you will be disconnected and will have to use another computer that is on the access control list to log in to the router.

8. Click **Apply** to save your Wireless Card Access List settings.

Now, only devices on this list can wirelessly connect to the wireless router.

> **Tip:** MAC address filtering adds an obstacle against unwanted access to your network, but NETGEAR recommends that you also use wireless security. Without wireless security, your trusted MAC addresses appear in your wireless transmissions, an intruder can read them and impersonate them.

Protecting Your Network

3

This chapter describes how to use the content filtering and reporting features of the wireless router to protect your network.

This chapter includes the following sections:

Protecting Access to Your Wireless Router

For security reasons, the wireless router has its own user name and password. Also, after a period of inactivity for a set length of time, the login automatically disconnects. You can use the following procedures to change the wireless router's password and the period for the administrator's login time-out.

Note: The user name and password are not the same as any other user name or password your might use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper case and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

Changing the Administrator Password

1. In the main menu, under Maintenance, select Set Password.

2. To change the password, first enter the old password, and then enter the new password twice.

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

   Note: *After changing the password, you are required to log in again to continue the configuration. If you have backed up the wireless router settings previously, you should do a new backup so that the saved settings file includes the new password.*

Set Password

Old Password

New Password

Repeat New Password

Apply   Cancel

Blocking Access to Internet Sites

The Wireless-N 150 Router WNR612v2 allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list.

Keyword application examples:

• If the keyword **XXX** is specified, the URL www.zzzyyqq.com/xxx.html is blocked.

• If the keyword **.com** is specified, only websites with other domain suffixes (such as .edu, .org, or .gov) can be viewed.

To block access to Internet sites:

1. Select Block Sites under Content Filtering in the main menu. The Block Sites screen displays.

2. Enable keyword blocking by selecting either **Per Schedule** or **Always**.

   To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see *Scheduling Blocking* on page 30.

   Block all access to Internet browsing during a scheduled period by entering a dot (**.**) as the keyword, and then set a schedule in the Schedule screen.

3. Add a keyword or domain by entering it in the keyword field and clicking **Add Keyword**. The keyword or domain name then appears the **Block sites containing these keywords or domain names** list.

   Delete a keyword or domain name by selecting it from the list and clicking **Delete Keyword**.

4. You can specify one trusted user, which is a computer that is exempt from blocking and logging. Specify a trusted user by entering that computer's IP address in the **Trusted IP Address** fields.

   Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address.

5. Click **Apply** to save all your settings in the Block Sites screen.

Blocking Access to Internet Services

The wireless router allows you to block computers on your network from using Internet services that you specify. This is called service blocking or port filtering. Services are 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 your network requests a service from a server computer on the Internet, it is identified by a service number or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet with destination port number 80 is an HTTP (Web server) request.

To block access to Internet services:

1. Select Block Services under Content Filtering in the main menu. The Block Services screen displays.

2. In the Services Blocking section of the screen, select either the **Per Schedule** or **Always** radio button, and then click **Apply**.

   To block by schedule, be sure to specify a time period in the Schedule screen (see *Scheduling Blocking* on page 30.)

To add Internet services you want to block:

1. On the Block Services screen, click **Add**.

2. The Block Services Setup screen displays.

3. From the **Service Type** list, select the application or service to be allowed or blocked.

4. To add a service or application to the **Service Type** list, select **User Defined**.

   • Find out which port number or range of numbers the application uses (these numbers often fall within the range 1024 to 65535). You can check the Internet Engineering Task Force (IETF) RFC1700, "Assigned Numbers," or contact the publisher of the application, or user groups.

   • Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both fields.

   • If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.

5. Select the radio button for the IP address configuration you want to block, and then enter the IP addresses in the appropriate fields.

6. Click **Add** to enable your Block Services Setup selections.

Blocking Services by IP Address Range

In the Filter Services For area, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Scheduling Blocking

The wireless router allows you to specify when blocking is enforced.

To schedule blocking:

1. Select **Schedule** under Content Filtering in the main menu. The Schedule screen displays.

2. Configure the schedule for blocking keywords and services.

   a. **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes. Select **Every Day** to select the check boxes for all days. Click **Apply**.

   b. **Time of Day to Block**. Select a start and end time in 24-hour format. Select **All Day** for 24-hour blocking. Click **Apply**.

   c. **Time Zone**. To verify and set the time zone:

      • **Time Zone**. To select your local time zone, use the drop-down list. This setting is used for the blocking schedule and for time-stamping log entries.

      • **Automatically Adjust for Daylight Savings Time**. If your region supports daylight savings time, select this check box. The router will automatically adjust the time at the start and end of the daylight savings time period.

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

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

Select **Logs** under Content Filtering in the main menu. The Logs screen displays.
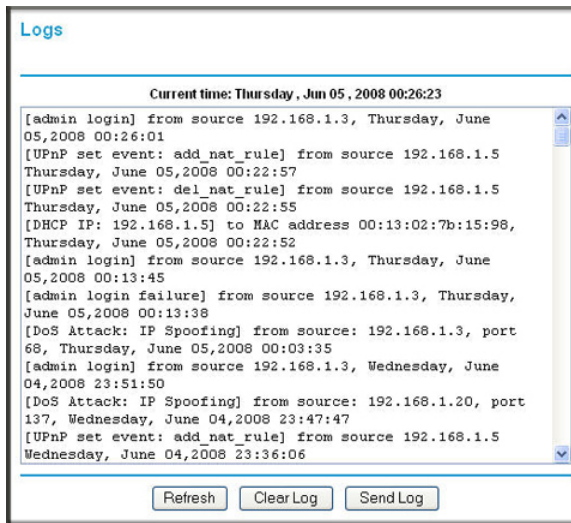
The following table describes the log entries.

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

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

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

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

Email Alerts and Web Access Log Notifications

To receive logs and alerts by email, you must provide your email account information.

To configure email alert and web access log notifications:

1. Select E-mail under Content Filtering in the main menu. The E-mail screen displays.

2. Select the **Turn E-mail Notification On** check box.

   a. Enter the name of your ISP's outgoing (SMTP) mail server (such as **mail.myISP.com**) in the **Your Outgoing Mail Server** field. You might be able to find this information in the configuration screen of your email program. If you leave this field blank, log and alert messages will not be sent by email.

   b. Enter the email address to which logs and alerts are sent in the **Send To This E-mail Address** field. This email address will also be used as the From address. If you leave this field blank, log and alert messages will not be sent by email.

3. If your e-mail server requires authentication, select the **My Mail Server requires authentication** check box.

   a. Enter your user name for the e-mail server in the **User Name** field.

   b. Enter your password for the e-mail server in the **Password** field.

4. You can specify that logs are automatically sent by e-mail with these options:

   • **Send alert immediately**. Select this check box for immediate notification of attempted access to a blocked site or service.

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

      - **Day**. Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.

      - **Time**. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

   If you select the Weekly, Daily, or Hourly option and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the Wireless Router's memory. If the Wireless Router cannot e-mail the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents.

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

So that the log entries are correctly time-stamped and sent at the correct time, be sure to set the time in the Scheduling screen (see *Scheduling Blocking* on page 30).

Customizing Your Network

4

This chapter describes how to configure advanced networking features of the wireless router, including LAN, WAN, and routing settings.

It contains the following sections:

- *Using the LAN IP Setup Options* on page 34"
- *Using a Dynamic DNS Service* on page 37
- *Configuring the WAN Setup Options* on page 38
- *Configuring Static Routes* on page 41

Using the LAN IP Setup Options

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP). To configure LAN IP settings, select LAN Setup under Advanced in the main menu. The LAN Setup screen displays.

Configuring a Device Name

The device name is a user-friendly name for the router. This name is shown in the Network on Windows Vista and the Network Explorer on all Windows systems. The **Device Name** field cannot be blank. The default name is WNR612v2.

Configuring LAN TCP/IP Setup Parameters

These are advanced settings that you might configure if you are a network administrator and your network contains multiple routers. The router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server (see *Using the Router as a DHCP Server* on page 35).

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

The router's default LAN IP configuration is:

• LAN IP address. **192.168.1.1**

- Subnet mask. **255.255.255.0**

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

The LAN IP settings are:

- **IP Address**. The LAN IP address of the router.
- **IP Subnet Mask**. The LAN subnet mask of the router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
- **RIP Direction**. RIP allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. **Both** is the default.
    - When set to **Both** or **In Only**, the router incorporates the RIP information that it receives.
    - When set to **Both** or **Out Only**, the router broadcasts its routing table periodically.
- **RIP Version**. This controls the format and the broadcasting method of the RIP packets sent by the router. (It recognizes both formats when receiving.) The default setting is **Disabled**.
    - **RIP-1** is universally supported. RIP-1 is usually adequate unless you have an unusual network setup.
    - **RIP-2B** carries more information than RIP-1 and uses subnet broadcasting.
    - **RIP-2M** carries more information than RIP-1 and uses multicasting.

Using the Router as a DHCP Server

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

> **Note:** For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. Click the link to the online document TCP/IP Networking Basics in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

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

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

• An IP address from the range you have defined

• Subnet mask

• Gateway IP address (the router's LAN IP address)

• Primary DNS server (if you entered a primary DNS address in the Basic Settings screen; otherwise, the router's LAN IP address)

• Secondary DNS server (if you entered a secondary DNS address in the Basic Settings screen)

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

Using Address Reservation

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

Address Reservation

#	IP Address	Device Name	MAC Address

Add | Edit | Delete

To reserve an IP address:

1. Click **Add**.

2. In the **IP Address** field, enter the IP address to assign to the computer or server. (Choose an IP address from the router's LAN subnet, such as **192.168.1.x**.)

3. Enter the MAC address of the computer or server.

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

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

   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 and force a DHCP release and renew.

To edit or delete a reserved address entry:

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

Using a Dynamic DNS Service

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

> **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.

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

Select **Dynamic DNS** under Advanced in the main menu. The Dynamic DNS screen displays.

Dynamic DNS

☐ Use a Dynamic DNS Service

Service Provider   www.DynDNS.org ▼
Host Name   [   ]
User Name   [   ]
Password   [   ]

☐ Use Wildcards

[Apply] [Cancel] [Show Status]

To configure for a Dynamic DNS service:

1. Register for an account with one of the Dynamic DNS service providers whose names appear in the **Service Provider** list. For example, for DynDNS.org, select **www.dynDNS.org**.

2. Select the **Use a Dynamic DNS Service** check box.

3. Select the name of your Dynamic DNS service provider.

4. Enter the host name (or domain name) that your Dynamic DNS service provider gave you.

5. Enter the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.

6. Enter the password (or key) for your Dynamic DNS account.

7. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature.
   For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.

8. Click **Apply** to save your configuration.

Configuring the WAN Setup Options

The WAN Setup options let you do the following:

- Disable Port Scan and DoS Protection.

- Configure a DMZ (demilitarized zone) server.

- Enable the wireless router to respond to a ping on the WAN (Internet) port.

- Disable IGMP Proxying – The IGMP Proxying function lets a LAN PC receive the multicast traffic is interested in from the Internet. You can click this check box to disable the function if you do not need it.

- Change the Maximum Transmit Unit (MTU) size.

- Disable DIP ALG – Some SIP applications have their own way to work around the NAT firewall issue, and the SIP ALG would conflict with those solutions. In most cases, you do not have to disable the SIP ALG. However, if your SIP applications cannot work with the router, you can disable the SIP ALG and try the applications again. Click the check box to disable SIP ALG.

- Enable IPv6 Pass-Through – IPv6 pass-through is disabled by default. If you have IPv6 capable devices in your configuration and would like to use IPv6 instead of IPv4, you can click this check box to enable IPv6 Pass)-Through.

Select **WAN Setup** under Advanced in the main menu. The WAN Setup screen displays.

Disabling Port Scan and DOS Protection

The Port Scan and DOS Protection feature protects your network and computers against attacks and intrusions. A stateful packet firewall carefully inspects incoming traffic packets, looking for known exploits such as malformed, oversized, or out-of-sequence packets. The Port Scan and Dos Protection feature should be disabled only in special circumstances, such as when you are troubleshooting application issues.

Setting Up a Default DMZ Server

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

WARNING!

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

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

The WAN Setup screen lets you configure a default DMZ server.

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

1. Select the **Default DMZ Server** check box.
2. In the **Default DMZ Server** fields, enter the IP address for that computer or server.
3. Click **Apply**.

Responding to a Ping on the Internet (WAN) Port

If you want the router to respond to a ping from the Internet, select the **Respond to Ping on Internet Port** check box. This should be used only as a diagnostic tool, since it allows your router to be discovered by Internet scanners. Do not select this check box unless you have a specific reason to do so, such as when troubleshooting your connection.

Setting the MTU Size

The normal MTU value for most Ethernet networks is 1500 bytes, 1492 bytes for PPPoE connections, or 1450 for PPTP connections. For some ISPs, you might need to reduce the MTU size, but this is rarely required and should not be done unless you are sure it is necessary for your ISP connection.

To change the MTU size:

1. In the **MTU Size** field, enter a new size between 64 and 1500.
2. Click **Apply** to save the new configuration.

Disabling IGMP Proxying

The IGMP Proxying function lets a LAN PC receive the multicast traffic it is interested in from the Internet. If you do not need this function, you can click the Disable IGMP Proxying check box to disable this function.

Disabling SIP ALG

Some SIP applications have their own way to work around the NAT firewall issue, and the SIP ALG would conflict with those solutions. In most cases, you do not have to disable the SIP ALG. However, if your SIP applications cannot work with the router, you can disable the SIP ALG and try the applications again. To disable SIP ALG, click the **Disable SIP ALG** check box.

Enabling IPv6 Pass-Through

IPv6 pass-through is disabled by default. If you have IPv6-capable devices in your configuration and would like to use those devices instead of IPv4, you can click the Enable IPv6 Pass-Through check box to enable the IPv6 Pass-Through function.

Configuring NAT Filtering

Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function. For more information about NAT, see *How Your Computer Accesses the Internet through Your Router* on page 54.

To change the NAT option:

1. In the NAT Filtering area, select either the **Secured** or the **Open** radio button.
2. Click **Apply** to save the new configuration.

Configuring Static Routes

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

As an example of when a static route is needed, consider the following case:

* Your primary Internet access is through a cable modem to an ISP.
* You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.
* Your company's network address is 134.177.0.0.

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

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

In this example:

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

To add or edit a static route:

1. Select **Static Routes** under Advanced in the main menu. The Static Routes screen displays.

Static Routes

#	Active	Name	Destination	Gateway

[Add] [Edit] [Delete]

2. Click **Add** to expand the Static Routes screen.

Static Routes

Route Name [   ]

☐ Private
☑ Active

Destination IP Address [   ] . [   ] . [   ] . [   ]
IP Subnet Mask [   ] . [   ] . [   ] . [   ]
Gateway IP Address [   ] . [   ] . [   ] . [   ]
Metric [   ]

[Apply] [Cancel]

3. In the **Route Name** field, enter a name for this static route. (This is for identification purposes only.)

4. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.

5. Select the **Active** check box to make this route effective.

6. In the **Destination IP Address** field, enter the IP address of the final destination.

7. In the **IP Subnet Mask** field, enter the IP subnet mask for this destination.
   If the destination is a single host, enter **255.255.255.255**.

8. In the **Gateway IP Address** field, enter the gateway IP address, which must be a router on the same LAN segment as the Wireless-N 150 Router WNR612v2.

9. In the **Metric** field, enter a number between 1 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, but if this is a direct connection, set it to 1.

10. Click **Apply** to have the static route entered into the table.

Maintenance

5

This chapter describes how to use the maintenance features of your wireless router.

This chapter includes the following sections:

Upgrading the Firmware

The wireless router's firmware (routing software) is stored in flash memory. By default, when you log in to your wireless router, it automatically checks the NETGEAR website for new firmware and alerts you if there is a newer version.
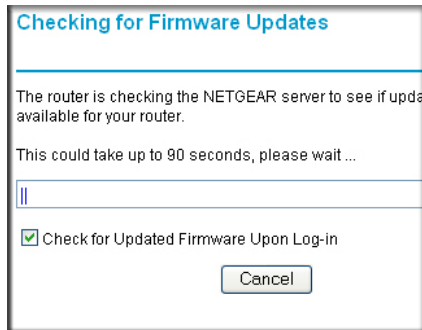
> **Note:** To turn off the automatic firmware check at log in, clear the **Check for Updated Firmware Upon Log-in** check box on the Router Upgrade screen.

If the wireless router discovers a newer version of firmware, the message on the left displays. If no new firmware is available, the message on the right displays.
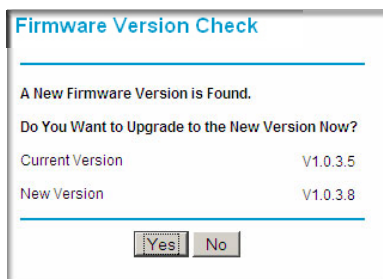
To upgrade, click **Yes** to allow the wireless router to download and install the new firmware.

⚠️ **WARNING!**

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

When the upload is complete, your wireless router automatically restarts. The upgrade process could take a few minutes. Read the new firmware release notes to determine whether you must reconfigure the wireless router after upgrading.

Manually Checking for Firmware Upgrades

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

Note: You can also check for upgrades from the NETGEAR website at *http://www.netgear.com/support*.

To manually check for new firmware and install it on your wireless router:

1. Under Maintenance on the wireless router main menu, select Router Upgrade.

2. Click **Browse**, and locate the firmware you downloaded (the file ends in .img or .chk).
3. Click **Upload** to send the firmware to the wireless router.

WARNING!

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

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

Backing Up, Restoring, and Erasing Your Settings

The configuration settings of the wireless router are stored in a configuration file. This file can be backed up to your computer, restored, or reverted to factory default settings. The following procedures explains how to do these tasks.

Backing Up the Configuration to a File

1. From the main menu, under Maintenance, select Backup Settings to display this screen:
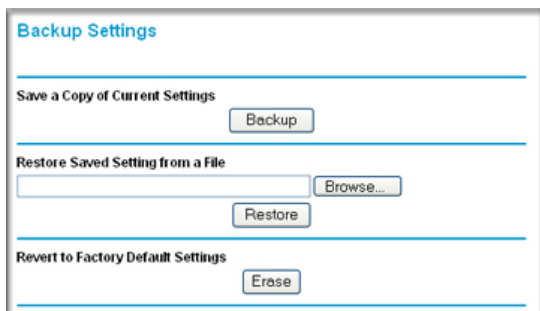
2. Click **Backup** to save a copy of the current settings.
3. Store the .cfg file on a computer on your network.

Restoring the Configuration from a File

1. In the main menu, under Maintenance, select Backup Settings.
2. Enter the full path to the file on your network, or click the **Browse** button to locate the file.
3. When you have located the .cfg file, click the **Restore** button to upload the file to the wireless router.
4. The wireless router then reboots automatically.

Erasing the Configuration

Sometimes you might want to restore the wireless router to the factory default settings. You can do this by using the erase function.

1. In the main menu, under Maintenance, select Backup Setting, and click the **Erase** button.
2. The wireless router then reboots automatically.

    After an erase, the wireless router's password is **password**, the LAN IP address is **192.168.1.1**, and the wireless router's DHCP client is enabled.

Note: To restore the factory default configuration settings when you do not know the login password or IP address, press the Restore Factory Settings button on the bottom of the wireless router for 6 seconds.

Viewing Wireless Router Status Information

To view router status and usage information, select Router Status under Maintenance in the main menu. The Router Status screen displays.

The following table describes the router status fields.

Table 3. Router Status Screen Fields

Field		Description
Hardware Version		The hardware version of the router.
Firmware Version		The wireless router firmware version.
GUI Language Version		The version of the GUI language.
Internet Port	MAC Address	The Ethernet MAC address being used by the Internet (ADSL) port.
	IP Address	The IP address used by the Internet (ADSL) port. If no address is shown, the wireless router cannot connect to the Internet.
	Internet	Type of Internet connection, such as DHCP.
	IP Subnet Mask	The IP subnet mask used by the Internet (ADSL) port.
	Domain Name Server	The DNS server IP addresses used by the wireless router. These addresses are usually obtained dynamically from the ISP.

Table 3. Router Status Screen Fields (Continued)

Field		Description
LAN Port	MAC Address	This field displays the Ethernet MAC address being used by the local (LAN) port of the wireless router.
	IP Address	This field displays the IP address being used by the local (LAN) port of the wireless router. The default is 192.168.1.1.
	DHCP	If Off, the wireless router does not assign IP addresses to PCs on the LAN. If On, the wireless router does assign IP addresses to PCs on the LAN.
	IP Subnet Mask	This field displays the IP subnet mask used by the local (LAN) port of the wireless router. The default is 255.255.255.0.
Wireless Port	Name (SSID)	The service set ID, also known as the wireless network name for WLAN1.
	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 for WLAN1. If disabled, the Wireless LED on the front panel is off.
	Broadcast Name	Indicates if the wireless router is configured to broadcast its SSID for WLAN1.
	Wi-Fi Protected Setup	Indicates whether the router's PIN is enabled and whether the router is configured for WPS (Wi-Fi Protected Setup). For more information, see *Using Push 'N' Connect (WPS) to Configure Your Wireless Network* on page 18.

Viewing Statistics

On the Router Status screen, click the **Show Statistics** button to display wireless router usage statistics, as shown in the following screen.

System Up Time 22:59:14							
Port	**Status**	**TxPkts**	**RxPkts**	**Collisions**	**Tx B/s**	**Rx B/s**	**Up Time**
WAN	100M/Full	190379	710681	0	1104	2160	22:58:51
LAN 1	Link down	374501	384019	0	2375	2001	22:14:55
LAN 2	100M/Full						05:14:55
WLAN	150M	20601	19681	0	475	160	22:59:10

Poll Interval : 5 (secs)   Set Interval   Stop

The Show Statistics screen displays the following statistics:

Table 4. Router Statistics Fields

Field	Description
WAN, LAN, or WLAN	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.

Table 4. Router Statistics Fields (Continued)

Field	Description
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
Rx B/s	The average line utilization for this port.
Up Time	The time elapsed since the last power cycle or reset.
Status	The link status of the port.

Viewing the Connection Status

On the Router Status screen, click the **Connection Status** button to display wireless router connection status.

This screen shows the following statistics:

Table 5. Connection Status Fields (PPPoE Network Type Example)

Field	Description
Connection Time	The time elapsed since the last connection to the Internet through the ADSL port.
Connecting to sender	The connection status.
Negotiation	Success or Failed.
Authentication	Success or Failed.

Table 5. Connection Status Fields (PPPoE Network Type Example)

Field	Description
Obtaining IP Address	The IP address assigned to the WAN port by the ADSL Internet Service Provider.
Obtaining Network Mask	The network mask assigned to the WAN port by the ADSL Internet Service Provider.

Viewing a List of Attached Devices

The Attached Devices screen contains a table of all IP devices that the router has discovered on the local network. Select Attached Devices under Maintenance in the main menu to view the table.

For each device, the table shows the IP address, NetBIOS host name or device name (if available), and the Ethernet MAC address. To force the router to look for attached devices, click **Refresh**.

Note: If the wireless router is rebooted, the table data is lost until the router rediscovers the devices.

Enabling Remote Management Access

Using the Remote Management feature, you can allow a user on the Internet to configure, upgrade, and check the status of your wireless router. Select Remote Management under Advanced in the main menu. The Remote Management screen displays.

Remote Management

☐ Turn Remote Management On

Remote Management Address:
10.1.32.90:8080

Allow Remote Access By:

○ Only This Computer: ☐ . ☐ . ☐ . ☐

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

◉ Everyone

Port Number: 8080

[Apply] [Cancel]

Note: Be sure to change the router's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

To configure your router for remote management:

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

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

Traffic Meter

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

To monitor traffic on your router:

1. Under the Advanced heading, select Traffic Meter.

2. To enable the Traffic Meter, click the **Enable Traffic Meter** check box.

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

   • No Limit – No restriction is applied when the traffic limit is reached.

   • Download only – The restriction is applied to incoming traffic only.

   • Both Directions – The restriction is applied to both incoming and outgoing traffic.

4. You can limit the amount of data traffic allowed per month:

   • By specifying how many Mbytes per month are allowed.

   • By specifying how many hours of traffic are allowed.

5. Set the **Traffic Counter** to begin at a specific time and date.

6. Set up **Traffic Control** to issue a warning message before the month limit of Mbytes or Hours is reached. You can select one of the following to occur when the limit is attained:

   • The Internet LED flashes green or amber.

   • The Internet connection is disconnected and disabled.

7. Set up **Internet Traffic Statistics** to monitor the data traffic.

8. Click the **Traffic Status** button if you want a live update on Internet traffic status on your router.

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

Fine-Tuning Your Network

6

This chapter describes how to modify the configuration of the wireless router to allow specific applications to access the Internet or to be accessed from the Internet, and how to make adjustments to enhance your network's performance.

This chapter includes the following sections:

Allowing Inbound Connections to Your Network

By default, the wireless router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. However, you might need to create exceptions to this rule for the following purposes:

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

Your router provides two features for creating these exceptions: port forwarding and port triggering. This section explains how a normal outbound connection works, followed by two examples explaining how port forwarding and port triggering operate and how they differ.

How Your Computer Accesses the Internet through Your Router

To access a computer on the Internet, your computer sends the router a message containing source and destination address and process information. Your router modifies the source information and creates and tracks 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 an Internet browser such as Internet Explorer. Invisible to you, your operating system assigns a service number (port number) to every communication process running on your computer. In this example, let's say Windows assigns port number 5678 to this browser session.

2. You select a Web page such as www.example.com. Your computer composes a Web page request message with the following address and port information:
   * The source address is your computer's IP address.
   * The source port number is 5678, the browser session.
   * The destination address is the IP address of www.example.com, which your computer finds by asking a DNS server.
   * The destination port number is 80, the standard port number for a Web server process.

   Your computer sends this request message to your router.

3. Your router creates an entry in its session table describing this communication session between your computer and the Web server at 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 router replaces the source address (your computer's private IP address) with it's public IP address. 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 source address is the IP address of www.example.com.
   - The source port number is 80, the standard port number for a Web server process.
   - The destination address is the public IP address of your router.
   - The destination port number is 33333.

   The Web server then sends this reply message to your router.

5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message, restoring the original address information replaced by NAT. The message now contains the following address and port information:
   - The source address is the IP address of www.example.com.
   - The source port number is 80, the standard port number for a Web server process.
   - The destination address is your computer's IP address.
   - The destination port number is 5678, the browser session that made the initial request.

   Your router sends this reply message to your computer, which displays the Web page from www.example.com.

6. When you finish your browser session, your router eventually senses 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.

How Port Triggering Changes the Communication Process

Usually, during an Internet session your computer sends outbound requests. The router sends replies to same port number where the session is. Replies to a different port number, are discarded. However, some application servers (such as FTP and IRC servers) send replies to multiple port numbers. With port triggering, you can tell the router to open more incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program, beginning a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

4. Noting your port triggering rule, and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.

5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, let's say port 33333) as the destination port. The IRC server also sends an "identify" message to your router with destination port 113.

6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.

7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.

8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

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

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

How Port Forwarding Changes the Communication Process

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

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

1. The user of a remote computer opens Internet Explorer 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:

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

   • The destination port number is 80, the standard port number for a Web server process.

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

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

   The destination address is replaced with 192.168.1.123.

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

3. Your Web server at 192.168.1.123 receives the request and composes a return message with the requested Web page data. Your Web server then sends this reply message to your router.

4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the Web page from www.example.com.

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

How Port Forwarding Differs from Port Triggering

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

• Port triggering can be used by any computer on your network, although only one computer can use it at a time.

• Port forwarding is configured for a single computer on your network.

• Port triggering does not need to know the computer's IP address in advance. The IP address is captured automatically.

• Port forwarding requires that you specify the computer's IP address during configuration, and the IP address must never change.

• Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.

• Port forwarding is always active and does not need to be triggered.

Configuring Port Forwarding to Local Servers

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

Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded. The DMZ server is configured in the WAN Setup screen, as discussed in *Setting Up a Default DMZ Server* on page 39.

Before starting, you need to determine which type of service, application, or game you will provide, and the local IP address of the computer that will provide the service. Be sure the computer's IP address never changes.

> **Tip:** To ensure that your server computer always has the same IP address, use the reserved IP address feature of your wireless router. See *Using Address Reservation* on page 36.

To configure port forwarding to a local server:

1. Select Port Forwarding/Port Triggering under Advanced in the main menu. The Port Forwarding/Port Triggering screen displays.

2. From the **Service Name** list, select the service or game that you will host on your network. If it is not in the list, see the following section, Adding a Custom Service."

3. In the corresponding **Server IP Address** fields, enter the last digit of the IP address of your local computer that will provide this service.

4. To the right of Server IP Address, click **Add**. The service appears in the list in the screen.

Adding a Custom Service

To define a service, game, or application that does not appear in the **Service Name** list, you must first find out which port number or range of numbers is used by the application. You can contact the publisher of the application or user groups or news groups.

To add a custom service:

1. Select Port Forwarding/Port Triggering under Advanced in the main menu.
2. Click **Add Service**. The Ports–Custom Services screen displays.

Ports - Custom Services

Service Name	
Service Type	TCP/UDP
Starting Port	(1~65534)
Ending Port	(1~65534)
Server IP Address	192 . 168 . 1 . 5

Apply   Cancel

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

Editing or Deleting a Port Forwarding Entry

To edit or delete a port forwarding entry:

1. In the table, select the button next to the service name.

	#	Server Name	Start Port	End Port	Server IP Address
○	1	FTP	20	21	192.168.1.2

Edit Service   Delete Service

2. Click **Edit Service** or **Delete Service** to make changes.
3. Click **Apply**.

Application Example: Making a Local Web Server Public

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

To make a local Web server public:

1. Assign your Web server either a fixed IP address or a dynamic IP address using DHCP address reservation, as explained in *Using Address Reservation* on page 36. In this example, your router will always give your Web server an IP address of 192.168.1.33.

2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your Web server at **192.168.1.33**.
    HTTP (port 80) is the standard protocol for Web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name as described in *Using the Router as a DHCP Server* on page 35.
    To access your Web server from the Internet, a remote user must know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Configuring Port Triggering

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

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

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

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

> **Note:** If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP). See *Using Universal Plug and Play* on page 62.

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

To set up port triggering:

1. Select Port Forwarding/Port Triggering under Advanced in the main menu. The Forwarding/Port Triggering screen displays.

2. Select the **Port Triggering** radio button. The port triggering information displays.

3. Clear the **Disable Port Triggering** check box.

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

---

4. In the **Port Triggering Timeout** field, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

5. Click **Add**. the Port Triggering–Services screen displays.

6. In the **Service Name** field, enter a descriptive service name.

7. In the **Service User** field, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.

8. Select the service type, either **TCP** or **UDP**.

9. In the **Triggering Port** field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.

10. Enter the inbound connection port information in the **Connection Type**, **Starting Port**, and **Ending Port** fields.

11. Click **Apply**. The service appears in the Port Triggering Portmap table.

Using Universal Plug and Play

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

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

To turn on Universal Plug and Play:

1. Select **UPnP** under Advanced the main menu. The UPnP screen displays.

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

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

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

   • **Advertisement Time To Live**. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value.

   • **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

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

Changing the MTU Size

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

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

• You have problems connecting to your ISP, or other Internet service, and either the technical support of the ISP or of NETGEAR recommends changing the MTU size. These might require an MTU change:

   - A secure website that will not open, or displays only part of a Web page

   - Yahoo email

   - MSN

   - America Online's DSL service

• You use VPN and have severe performance problems.

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

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

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

Table 6. Common MTU Sizes

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

To change the MTU size:

1. In the main menu, under Advanced, select **WAN Setup**.
2. In the **MTU Size** field, enter a new size between 64 and 1500.
3. Click **Apply** to save the new configuration.

Quality of Service

Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The Wireless-N 150 Router WNR612v2 can provide QoS prioritization over the wireless link and on the Internet connection.

Using WMM QoS for Wireless Multimedia Applications

The Wireless-N 150 Router WNR612v2 supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must be WMM enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

Configuring QoS for Internet Access

To specify prioritization of traffic, you must create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen.

To create a QoS policy:

From the main menu, under Advanced, select QoS Setup. The QoS Setup screen displays:

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

QoS for Applications and Online Gaming

To create a QoS policy for traffic for specific applications or online games:

1. From the main menu of the browser interface, under Advanced, select QoS Setup. The QoS Setup screen displays.

2. On the QoS Setup screen, click **Setup QoS rule**. The QoS - Priority Rules screen displays.

Qos Priority Rule list

	#	QoS Policy	Priority	Description
○	1	MSN_messenger	High	MSN_messenger application
○	2	Skype	Highest	Skype application
○	3	Yahoo_Messanger	High	Yahoo_messanger application
○	4	IP_Phone	Highest	IP_Phone application
○	5	Vonage_IP_Phone	Highest	Vonage_IP_Phone application
○	6	NetMeeting	High	Netmeeting application
○	7	AIM	High	AIM application
○	8	Google_Talk	Highest	Google_Talk application
○	9	Counter Strike	High	On-line Gaming Counter Strike
○	10	Age of Empires	High	On-line Gaming Age of Empires
○	11	Diablo II	High	On-line Gaming Diablo II
○	12	Everquest	High	On-line Gaming Everquest
○	13	Half Life	High	On-line Gaming Half Life
○	14	Quake 2	High	On-line Gaming Quake 2
○	15	Quake 3	High	On-line Gaming Quake 3
○	16	Unreal Tourment	High	On-line Gaming Unreal Tourment
○	17	Warcraft	High	On-line Gaming Warcraft
○	18	Return to Castle Wolfenstein	High	On-line Gaming Return to Castle Wolfenstein

Edit   Delete   Delete All

Add Priority Rule

Apply   Cancel

For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

3. Click **Add Priority Rule**. The QoS - Priority Rules screen displays.

QoS - Priority rules

Priority

QoS Policy for   MSN Messenger

Priority Category   Applications

Applications   MSN Messenger

Priority   Normal

Apply   Cancel

4. In the **QoS Priority** field, select either **Applications** or **Online Gaming**. In either case, a list of predefined applications or games displays in the **Applications** drop-down list.

5. From the **Applications** list, you can select an existing item, or you can scroll to the bottom of the list and select **Add a New Application** or **Add a New Game**.

a. If you chose to add a new entry, the screen expands as shown:

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

c. Select the packet type, either **TCP, UDP,** or both (**TCP/UDP**), and specify the port number or range of port numbers used by the application or game.

6. From the **Priority** drop-down list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.

7. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

8. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.

9. Click **Apply**.

QoS for a Router LAN Port

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

1. On the QoS Setup screen, click **Setup QoS Rule**.

2. From the **Priority Category** list, select **Ethernet LAN Port**. The QoS - Priority Rules screen changes:

3. From the **LAN port** list, select the LAN port that will have a QoS policy.

4. From the **Priority** drop-down list, select the priority that this port's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.

5. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

6. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.

7. Click **Apply**.

QoS for a MAC Address

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

1. On the QoS Setup screen, click **Add Priority Rule**.

2. From the **Priority Category** list, select **MAC Address**. The QoS - Priority Rules screen changes:

3. If the device to be prioritized appears in the MAC Device List, select it. The information from the MAC Device List is used to populate the policy name, MAC Address, and Device Name fields. If the device does not appear in the MAC Device List, click **Refresh**. If it still does not appear, you must complete these fields manually.

4. From the **Priority** drop-down list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.

5. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

6. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.

7. Click **Apply**.

Editing or Deleting an Existing QoS Policy

To edit or delete an existing QoS policy:

1. On the QoS Setup screen, select the radio button next to the QoS policy to be edited or deleted

	#	QoS Policy	Priority	Description
○	1	MSN messenger	High	MSN_messenger Applications
○	2	Yahoo Messenger	High	Yahoo_messenger Applications
○	3	IP Phone	Highest	IP_Phone Applications
○	4	Vonage IP Phone	Highest	Vonage_IP_Phone Applications
○	5	NetMeeting	High	Netmeeting Applications
○	6	AIM	High	AIM Applications
○	7	Google Talk	Highest	Google_Talk Applications
○	8	Netgear EVA	Highest	Netgear_EVA Applications
○	9	Counter Strike	High	On-line Gaming Counter Strike
○	10	Age of Empires	High	On-line Gaming Age of Empires
○	11	Everquest	High	On-line Gaming Everquest
○	12	Quake 2	High	On-line Gaming Quake 2
○	13	Quake 3	High	On-line Gaming Quake 3
○	14	Unreal Tourment	High	On-line Gaming Unreal Tourment
○	15	Warcraft	High	On-line Gaming Warcraft

Edit Delete   Delete All
Add Priority Rule

Apply Cancel

2. Do one of the following:

   • Click **Delete** to remove the QoS policy.

   • Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.

3. Click **Apply** in the QoS Setup screen to save your changes.

Overview of Home and Small Office Networking Technologies

Common connection types and their speed and security considerations are:

• **Broadband Internet**. Your Internet connection speed is determined by your modem type, such as ADSL or cable modem, as well as the connection speed of the sites to which you connect, and general Internet traffic. ADSL and cable modem connections are asymmetrical, meaning they have a lower data rate *to* the Internet (upstream) than *from* the Internet (downstream). Keep in mind that when you connect to another site that also has an asymmetrical connection, the data rate between your sites is limited by each side's upstream data rate. A typical residential ADSL or cable modem connection provides a downstream throughput of about 1 to 3 megabits per second (Mbps). Newer technologies such as ADSL2+ and Fiber to the Home (FTTH) will increase the connection speed to tens of Mbps.

- **Wireless**. Your Wireless-N 150 Router WNR612v2 provides a wireless data throughput of up to 150 Mbps. With the introduction of the newer WPA and WPA2 encryption and authentication protocols, wireless security is extremely strong.

  To get the best performance, use RangeMax NEXT adapters such as the WN511B for your computers. Although the wireless router is compatible with older 802.11b and 802.11g adapters, the use of these older wireless technologies in your network can result in lower throughput overall (typically less than 10 Mbps for 802.11b and less than 40 Mbps for 802.11g). In addition, many older wireless products do not support the latest security protocols, WPA and WPA2.

- **Powerline**. For connecting rooms or floors that are blocked by obstructions or are distant vertically, consider networking over your building's AC wiring. NETGEAR's Powerline HD family of products delivers up to 200 Mbps to any outlet, while the older-generation XE family of products delivers 14 Mbps or 85 Mbps. Data transmissions are encrypted for security, and you can configure an individual network password to prevent neighbors from connecting.

  The Powerline HD family of products can coexist on the same network with older-generation XE family products or HomePlug 1.0 products, but they are not interoperable with these older products.

- **Wired Ethernet**. As gigabit-speed Ethernet ports (10/100/1000 Mbps) become common on newer computers, wired Ethernet remains a good choice for speed, economy, and security. Gigabit Ethernet can extend up to 100 meters with twisted-pair wiring of Cat 5e or better. A wired connection is not susceptible to interference, and eavesdropping would require a physical connection to your network.

> **Note:** Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, can lower actual data throughput rate.

Assessing Your Speed Requirements

Because your Internet connection is likely to operate at a much lower speed than your local network, faster local networking technologies might not improve your Internet experience. However, many emerging home applications require high data rates. For example:

- Streaming HD video requires 10 to 30 Mbps per stream. Because latency and packet loss can disrupt your video, plan to provide at least twice the capacity you need.

- Streaming MP3 audio requires less than 1 Mbps per stream and does not strain most modern networks. Like video, however, streaming audio is also sensitive to latency and packet loss, so a congested network or a noisy link can cause problems.

- Backing up computers over the network has become popular due to the availability of inexpensive mass storage. The following table shows the time to transfer 1 gigabyte of data using various networking technologies.

Table 7. Theoretical Transfer Time for 1 Gigabyte

Network Connection	Theoretical Raw Transfer Time
Gigabit wired Ethernet	8 seconds
RangeMax NEXT Wireless-N	26 seconds
Powerline HD	40 seconds
100 Mbps wired Ethernet	80 seconds
802.11n wireless	45 seconds
802.11g wireless	150 seconds
802.11b wireless	700 seconds
10 Mbps wired Ethernet	800 seconds
Cable modem (3 Mbps)	2700 seconds
Analog modem (56 kbps)	144,000 seconds (40 hours)

Troubleshooting

7

This chapter provides information about troubleshooting your wireless router. After each problem description, instructions are provided to help you diagnose and solve the problem. As a first step, review the Quick Tips.

> **Tip:** NETGEAR provides helpful articles, documentation, and the latest software updates at *http://www.netgear.com/support*.

This chapter includes the following sections:

Quick Tips

This section describes tips for troubleshooting some common problems:

Be sure to restart your network in this sequence.

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

Make sure that the Ethernet cables are securely plugged in.

- The Internet status light on the wireless router is on if the Ethernet cable connecting the wireless router and the modem is plugged in securely and the modem and wireless router are turned on.

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

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

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

- If you have enabled the wireless router to restrict wireless access by MAC address, you must add the wireless computer's MAC address to the router's wireless card access list.

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

- LAN connected computers must be configured to obtain an IP address automatically using DHCP. For more information, see the links in Appendix B.

- Some cable modem services require you to use the MAC address of the computer registered on the account. If so, in the Router MAC Address section of the Basic Settings menu, select **Use this Computer's MAC Address**. Click **Apply** to save your settings. Restart the network in the correct sequence.

Check the Power/Test light to verify correct router operation.

If the Power/Test light blinks green within 2 minutes after you turn the router on, reset the router according to the instructions in *Restoring the Default Configuration and Password* on page 80.

Troubleshooting Basic Functions

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

1. When power is first applied, verify that the Power/Test light ⚒ is on.

2. Verify that the Power/Test light turns green and blinks slowly, indicating that the self-test procedure is running.

3. After approximately 20 seconds, verify that:

   a. The color of the Power/Test light changes to solid green.

   b. The LAN port lights are lit for any local ports that are connected.

      If a port's light is lit, a link has been established to the connected device. If a LAN port is connected to a 10 or 100 Mbps device, verify that the port's light is green.

   c. The Internet port is connected and its light is lit.

If the correct behavior does not occur, see the appropriate following section.

The Power/Test light is not on.

If the Power/Test and other lights are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power adapter is properly connected to a functioning power outlet.

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

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

The Power/Test light blinks green slowly and continuously.

The router firmware is corrupted.

For help restoring your firmware, contact Technical Support.

The Internet or LAN port lights are not on.

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

1. Make sure that the Ethernet cable connections are secure at the router and at the computer.

2. Make sure that power is turned on to the connected computer.

3. Be sure you are using Ethernet cables like the cable that was supplied with the wireless router.

Login Problems

If you are unable to log in to the wireless router, check the following:

• If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the *NETGEAR Wireless Router Installation Guide*.

• Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that the Caps Lock is off when entering this information.

• Make sure your computer's IP address is on the same subnet as the router. If your are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254. Refer to your computer's documentation or see Preparing Your Network in Appendix B for help with configuring your computer.

Note: If your computer cannot reach a DHCP server, some operating systems will assign an IP address in the range 169.254.x.x. If your IP address is in this range, verify that you have a good connection from the computer to the router, then restart (reboot) your computer.

• If your router's IP address has been changed and you don't know the current IP address, reset the router's configuration to the factory defaults. This procedure will reset the router's IP address to 192.168.1.1 (see Factory Default Settings in Appendix A).

• Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded. Try closing the browser and reopening it again.

• If you are attempting to set up your NETGEAR router as an additional router behind an existing router in your network, consider replacing the existing router instead. NETGEAR does not support such a configuration.

• If you are attempting to set up your NETGEAR router as a replacement for an ADSL gateway in your network, the router cannot perform many gateway services, for example, converting ADSL or Cable data into Ethernet networking information. NETGEAR does not support such a configuration.

Checking the Internet Service Connection

If you can access your router, but your router is unable to access the Internet, review the topics in this section:

Obtaining an Internet IP Address

If your wireless router is unable to access the Internet, and your Internet light is amber, check the wireless router to see if it is able to get an Internet IP address from your service provider.

Unless you have a static IP address, your wireless router automatically requests an IP address from your service provider.

To check your wireless router's Internet IP address:

1. Log in to the wireless router.
2. Select **Router Status**, under Maintenance in the main menu, to check that an IP address is shown for the Internet Port. If 0.0.0.0 is shown, your wireless router has not obtained an IP address from your service provider.

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

• You might need to force your cable or DSL modem to recognize your new router by restarting your network, in the sequence described in the *NETGEAR Wireless Router Setup Manual.*

• Your service provider might require a login. Ask your service provider whether they require a PPP over Ethernet (PPPoE) login (see *Troubleshooting PPPoE* on page 76).

• You might have incorrectly set the service name, user name or password. Review your router's **Basic Settings** screen.

• Your service provider might check for your computer's host name. Assign the computer Host Name of your ISP account to the wireless router on the **Basic Settings** screen.

• Your service provider might only allow one Ethernet MAC address to connect to the Internet, and check for your computer's MAC address. If this is the case:

  - Inform your service provider that you have bought a new network device, and ask them to use the wireless router's MAC address, or

  - Configure your router to spoof your computer's MAC address. On the **Basic Settings** screen in the Router MAC Address section, select "Use this Computer's MAC Address" and click **Apply.** Then restart your network in the correct sequence (see the *NETGEAR Wireless Router Setup Manual* for instructions).

Troubleshooting PPPoE

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

To troubleshoot a PPPoE connection:

1. Log in to the wireless router.
2. Select **Router Status** under **Maintenance** on the main menu.
3. Click **Connection Status**. If all of the steps indicate "OK," then your PPPoE connection is up and working.

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

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

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

Troubleshooting Internet Browsing

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

- **Your computer might not recognize any DNS server addresses**. A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the wireless router's configuration, restart your computer. Alternatively, you can configure your computer manually with a DNS address, as explained in the documentation for your computer.

- **Your computer might not have the wireless router configured as its default gateway**. Reboot the computer and verify that the wireless router address (192.168.1.1) is listed by your computer as the default gateway address.

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

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

- When entering configuration settings, be sure to click **Apply** before moving to another screen or tab, or your changes could be lost.

- Click **Refresh** or **Reload** in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

Troubleshooting Your Network Using the Ping Utility

Most network devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a network is made very easy by using the ping utility in your computer or workstation. This section includes:

- Testing the LAN Path to Your Router"
- Testing the Path from Your Computer to a Remote Device"

Testing the LAN Path to Your Router

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

To ping the router from a running Windows PC:

1. From the Windows toolbar, click Start, and then select **Run**.

2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   `ping www.routerlogin.net`

3. Click **OK**.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

`Request timed out`

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

   - Wrong physical connections

     - For a wired connection, make sure that the numbered LAN port light is on for the port to which you are connected. If the light is off, follow the instructions in *Troubleshooting Basic Functions* on page 74.

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

   - Wrong network configuration

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

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

Testing the Path from Your Computer to a Remote Device

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

1. From the Windows toolbar, click the Start button, and then select **Run**.

2. In the Windows Run window, type:

   `ping -n 10 <IP address>`

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

If the path is functioning correctly, replies like those shown in the previous section are displayed. If you do not receive replies:

   - Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not be

visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in the online document you can access from Preparing Your Network in Appendix B.

- Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) is different from the network address of the remote device.

- Check that your cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your computer, enter that host name as the account name in the Basic Settings screen.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized computer.

Problems with Date and Time

Select **E-mail** under Content Filtering in the main menu to display a screen that shows the current date and time of day. The Wireless-N 150 Router WNR612v2 uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000.
  Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are correct. 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.
  Cause: The router does not adjust for daylight savings time. In the E-mail screen, select the **Automatically Adjust for Daylight Savings Time** check box.

Problems with Wireless Adapter Connections

If your wireless adapter is unable to connect, check its connection settings.

To check the adapter's connection settings:

1. Open the adapter setup utility to check connections:
   - **NETGEAR Smart Wizard utility**. If you installed a NETGEAR wireless adapter in your computer, a Smart Wizard utility program is installed that can provide helpful information about your wireless network. You can find this program in your Windows Program menu or as an icon in your system tray. Other wireless card manufacturers might include a similar program.

   - **Windows basic setup utility**. If you have no specific wireless card setup program installed, you can use the basic setup utility in Windows:

- Open the Windows Control Panel, and double-click **Network Connections**.

- In the LAN section, double-click **Wireless Network Connection**.

2. Use the adapter's setup program to scan for available wireless networks, looking for the network name (SSID) of **NETGEAR**, or your custom SSID if you have changed it.

3. If your wireless network appears and has good signal strength, configure and test with the simplest wireless connection possible.

If your wireless network does not appear, check these conditions:

- Is your router's wireless radio enabled? See *Advanced Wireless Settings* on page 22.

- Is your router's SSID broadcast enabled? See *Advanced Wireless Settings* on page 22.

- Is your router set to a wireless standard that is not supported by your wireless adapter? Check the Mode setting as described in *Manually Configuring Your Wireless Settings* on page 14.

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

- Is your router too far from your adapter, or too close? Place the computer that has the adapter near the router, but at least 6 feet away, and see whether the signal strength improves.

- Is your wireless signal obstructed by objects between the router and your adapter? See *Planning Your Wireless Network* on page 13.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings that reset the router's user name to **admin**, the password to **password**, and the IP address to **192.168.1.1**.

> ⚠️ **WARNING!**
>
> **These procedures erase all current configuration settings.**

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

- Use the Erase function of the router. To use the Erase function, see *Erasing the Configuration* on page 46.

- Use the restore factory settings button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

To use the restore settings button:

1. Locate the restore factory settings button on the rear panel of the router.

2. Use a sharp object such as a pen or a paper clip to press and hold the restore factory settings button for about 5 seconds, until the Power light begins to blink.

3. Release the restore factory settings button, and wait for the router to restart, and for the Power light to stop blinking and become solid green.

The factory default settings will be restored so that you can access the router from your Web browser using the factory defaults.

If the wireless router fails to restart, or the Power light continues to blink or turns solid amber, the unit might be defective. If the error persists, you might have a hardware problem and should contact Technical Support at *http://www.netgear.com/support*.

Factory Default Settings and Technical Specifications

A

Factory Default Settings

To return the router to its factory default settings, see *Restoring the Default Configuration and Password* on page 80. The following table shows the default settings.

Feature	Default Setting
Router Login	
Router Login URL	http://www.routerlogin.net *or* http://www.routerlogin.com
Login Name (case-sensitive) printed on product label	admin
Login Password (case-sensitive) printed on product label	password
Internet Connection	
WAN MAC Address	Default hardware address (on label)
MTU Size	1500
Local Network	
Router LAN IP address printed on product label (also known as Gateway IP address)	192.168.1.1
Router Subnet	255.255.255.0
DHCP Server	Enabled
DHCP range	192.168.1.2 to 192.168.1.254
Time Zone	GMT
Time Zone Adjusted for Daylight Saving Time	Disabled
Allow a Registrar to configure this router	Enabled

Feature	Default Setting
Wireless	
Wireless Communication	Enabled
SSID Name	NETGEAR
Security	Disabled
Wireless Access List (MAC Filtering)	All wireless stations allowed
Broadcast SSID	Enabled
Transmission Speed	Auto[1]
Country/Region	United States (North America only; otherwise varies by country and region)
RF Channel	Auto
Operating Mode	Up to 150 Mbps
Data Rate	Best
Output Power	Full
Firewall	
Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests except for traffic on port 80, the http port)
Outbound (communications going out to the Internet)	Enabled (all)

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.

General Specifications

Feature	General
Network Protocol and Standards Compatibility	
Data and Routing Protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, and UPnP
Power Adapter	
AC plug is localized	110V-220V, 50/60 Hz, input
All regions (output)	7.5V DC @ 1.0A, output
Physical	
Dimensions	141.5 x 94 x 30 mm (5.6 x 3.7 x 1.2 in.)
Weight	0.137 kg (0.302 lb)
Environmental	
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Designed to conform to the following standards	FCC Part 15 Class B EN 55022/24 (CISPR 22/24) Class B EN 60950 (CE LVD) Class B China CCC & SRRC Brazil ANATEL Russia GOST-R KCC
Interface Specifications	
LAN	10BASE-T or 100BASE-Tx, RJ-45
WAN	10BASE-T or 100BASE-Tx, RJ-45

Related Documents

B

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Windows XP and Vista Wireless Configuration Utilities Application Note	http://documentation.netgear.com/reference/enu/winzerocfg/index.htm
TCP/IP Networking Basics	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Networking Basics	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing Your Network	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN)	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm

Notification of Compliance

C

NETGEAR Wireless Routers, Gateways, AP's

Regulatory Compliance Information

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

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

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, Santa Clara, CA 95134, declare under our sole responsibility that the Product Name™/® & Model 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, (Product Name™/® & Model), 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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Interference Reduction Table

Household Appliance	Recommended Minimum Distance between NETGEAR equipment and household appliance to reduce interference (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

Europe – EU Declaration of Conformity

CE ①

Marking with the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC).

This equipment meets the following conformance standards:

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

• 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.

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

EDOC in Languages of the European Community

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.

Index