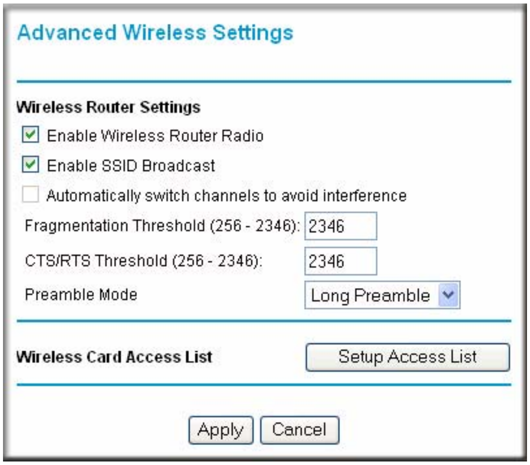
Chapter 8
Advanced Configuration of the Router

This chapter describes how to configure the advanced features of your RangeMax 240 Wireless Router WPNT834. These features can be found under the Advanced heading in the main menu of the browser interface.

➡	**Note:** If you are unfamiliar with networking and routing, see "Wireless Communications" in Appendix B, to become more familiar with the terms and procedures used in this chapter.

Configuring Advanced Wireless Settings

Click on **Wireless Settings** under the Advanced Heading in the main menu to display the Advanced Wireless Settings screen:



Advanced Wireless Settings

Wireless Router Settings

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

□ Automatically switch channels to avoid interference

Fragmentation Threshold (256 - 2346): 2346

CTS/RTS Threshold (256 - 2346): 2346

Preamble Mode: Long Preamble

Figure 8-1

⚠	**Warning:** The Wireless Router is already configured with the optimum settings. Do not alter these settings unless directed by NETGEAR support. Incorrect settings may disable the Wireless Router unexpectedly.

Program the advanced wireless settings as follows:

- **Enable Wireless Router Radio**—the Wireless Router Radio of this router can be enabled or disabled to allow wireless access. The wireless icon on the front of the router displays the current status of the Wireless Router Radio to let you know if it is disabled or enabled. If enabled, wireless stations will be able to access the Internet. If disabled, wireless stations will not be able to access the Internet.
- **Enable SSID Broadcast**—if enabled, the Wireless Router SSID will broadcast its name (SSID) to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.
- **Automatically switch channels to avoid interference.** If enabled, the WPNT834 router will periodically survey the wireless environment to ensure that it is using the clearest channel. If a clearer channel is available, it may automatically switch channels.

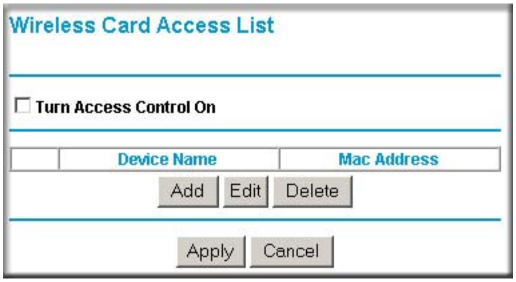
➡	**Note:** After the router switches channels, there may be a slight delay while your wirless computers reconnect to the router. If you want to avoid this possibility, leave this checkbox unselected.

- **Fragmentation Threshold, CTS/RTS Threshold, Preamble Mode**—these settings are reserved for wireless testing and advanced configuration only. Do not change these settings.
- **Wireless Card Access List**—by default, any wireless computer that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific computers based on their MAC addresses.

Wireless Card Access List

The Wireless Card Access Setup page displays a list of wireless computers that are allowed to connect to the router based on their MAC addresses. These wireless computers must also have the correct SSID and WEP settings configured on the Wireless Settings page to access the wireless network.

From the Advanced Wireless Settings menu, click the **Setup Access List** button to display the Wireless Access List menu:



Wireless Card Access List

☐ Turn Access Control On

	Device Name	Mac Address

Figure 8-2

Program the wireless card access list as follows:

1. Turn access control on:

- **a.** Click the **Turn Access Control On** check box to enable the restricting of wireless computers by their MAC addresses.
- **b.** Click the **Apply** button to save changes and return to the Wireless Settings page.

> **Note:** If Turn Access Control On is enabled and the Access Control List is blank; then no wireless computers will be able to connect to your wireless network.

2. Set Up The Access Control List:

- **a.** Click the **Add** button to go to the Access Setup menu (see Figure 8-3). This menu displays a list of currently active wireless cards and their Ethernet MAC addresses.
- **b.** If the desired computer appears in the list, you can click the radio button of that computer to capture its MAC address; otherwise, you can manually enter the MAC address of the authorized computer. The MAC address can usually be found on the bottom of the wireless device.

c. If no Device Name appears, you can type a descriptive name for the computer that you are adding.

d. When you have finished entering the MAC address, return to the Wireless Access List menu by clicking the **Add** button.

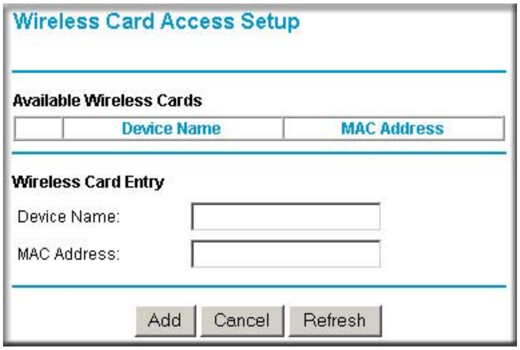
e. Repeat steps a - d for each wireless computer.

f. Click the **Turn Access Control On** box to enable Access Control.

g. Click the **Apply** button to save changes and return to the Wireless Settings page.

Wireless Card Access Setup

The Wireless Card Access Setup screen is invoked by clicking **Add** on the Wireless Card Access List menu (see "Wireless Card Access List" on page 8-3):



Wireless Card Access Setup

Available Wireless Cards

	Device Name	MAC Address

Wireless Card Entry

Device Name:

MAC Address:

Figure 8-3

Program the Wireless Card Access Setup menu as follows:

- **Available Wireless Cards**—the Available Wireless Cards list displays any available wireless computers and their MAC addresses.

  If the wireless computer appears in the Available Wireless Cards list, you can click on the radio button of that computer to capture its MAC address. If your wireless computer is not displayed, make sure that the computer is configured correctly, and then click on the **Refresh** button to update the available list of wireless computers. If the wireless computer is still not displayed, then follow the instructions below on how to manually setup the wireless computer's MAC address.

- **Wireless Card Entry**—if no wireless computers appear in the Available Wireless Cards list, you can manually enter the Device Name and MAC address of the authorized wireless computer.

> **Note:** The MAC address is a twelve character key containing the characters 0-9, A-F only and separated by colons (for example., 00:09:AB:CD:EF:01) that can usually be found on the bottom of the wireless device.

Configuring Port Triggering and Port Forwarding

Port Triggering is an advanced feature that can be used to easily enable gaming and other Internet applications. Port Forwarding is typically used to enable similar functionality, but it is static and has some limitations.

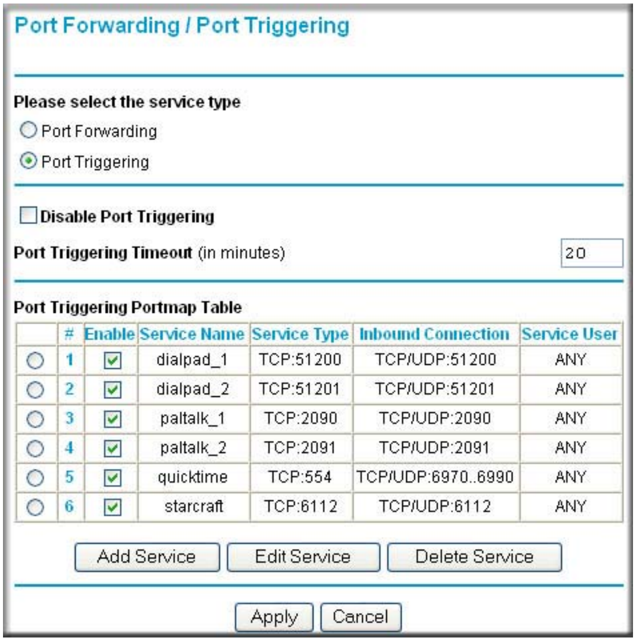
> **Note:** If you use applications such as multi-player gaming, peer-to-peer connections, real time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable UPnP according to the instructions at "Using Universal Plug and Play (UPnP)" on page 8-22.

Port Triggering opens an incoming port temporarily and does not require the server on the Internet to track your IP address if it is changed by DHCP, for example.

Port Triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and triggers the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

Using the Port Triggering page, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games (like Quake III), or to use Internet applications (like CUseeMe).

Port forwarding is designed for FTP, Web Server or other server-based services. Once port forwarding is set up, requests from the Internet will be forwarded to the proper server. Port triggering will only allow requests from the Internet after a designated port is 'triggered'. Port triggering applies to chat and Internet games.



Port Forwarding / Port Triggering

Please select the service type

○ Port Forwarding

● Port Triggering

□ Disable Port Triggering

Port Triggering Timeout (in minutes) 20

Port Triggering Portmap Table

	#	Enable	Service Name	Service Type	Inbound Connection	Service User
○	1	☑	dialpad_1	TCP:51200	TCP/UDP:51200	ANY
○	2	☑	dialpad_2	TCP:51201	TCP/UDP:51201	ANY
○	3	☑	paltalk_1	TCP:2090	TCP/UDP:2090	ANY
○	4	☑	paltalk_2	TCP:2091	TCP/UDP:2091	ANY
○	5	☑	quicktime	TCP:554	TCP/UDP:6970..6990	ANY
○	6	☑	starcraft	TCP:6112	TCP/UDP:6112	ANY

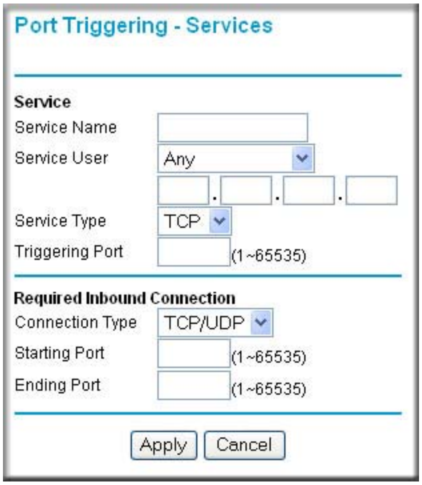
Figure 8-4

Note: If the Disable Port Triggering box is checked after configuring port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it will not be used.

- **Port Triggering Timeout**—Enter a value up to 9999 minutes. The Port Triggering Timeout value controls the inactivity timer for the designated inbound port(s). The inbound port(s) close when the inactivity timer expires.
- **For Internet Games or Applications**—Before starting, you need to know which service, application or game you will be configuring. Also, you need to have the outbound port (triggering port) address for this game or application.

Follow these steps to set up a computer to play Internet games or use Internet applications:

1. Select **Port Forwarding / Port Triggering** from the Advanced section of the main menu.
2. Select the service type by clicking the **Port Triggering** radio button. The Port Triggering screen is displayed as shown in Figure 8-4.
3. Click **Add Service**.



Port Triggering - Services

Service

Service Name

Service User: Any

Service Type: TCP

Triggering Port (1~65535)

Required Inbound Connection

Connection Type: TCP/UDP

Starting Port (1~65535)

Ending Port (1~65535)

Figure 8-5

4. Enter a service name in the Service Name box.
5. Under Service User, select **Any** (default) to allow this service to be used by everyone in your network. Otherwise, select **Single address** and enter the IP address of one computer to restrict the service to a particular computer.
6. Select the Service Type.
7. Enter the outbound port number in **Triggering Port** box.
8. Enter the inbound connection port information such as Connection Type, Starting Port and Ending Port boxes. This information can be obtained from the game or applications manual or the product's support Web site.
9. Click **Apply** to save your changes.

Configuring Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make a local server (for example, a Web server or game server) visible and available to the Internet. This is done using the Port Forwarding menu.

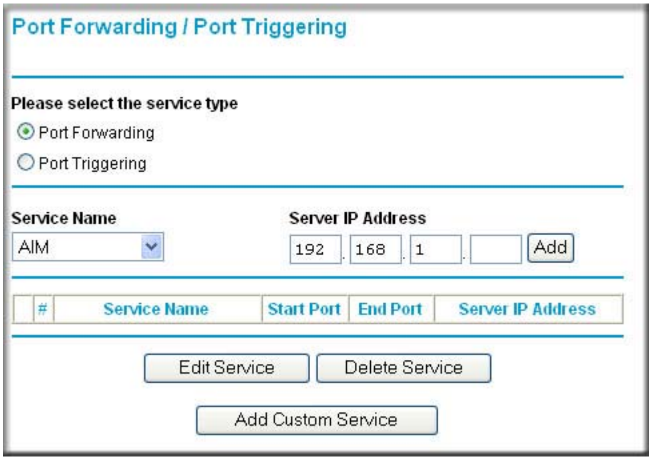
Use the Port Forwarding menu to configure the router to forward incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the WAN Setup menu as discussed in "Configuring the WAN Setup Options" on page 8-11.

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

Note: To assure that the same computer always has the same IP address, use the reserved IP address feature of your WPNT834 router. See "Using Address Reservation" on page 8-15 for instructions on how to use reserved IP addresses.

To configure port forwarding to a local server:

1. From the main menu of the browser interface, under Advanced, click on **Port Forwarding / Port Triggering** to view the port forwarding menu, shown below.



Port Forwarding / Port Triggering

Please select the service type

● Port Forwarding

○ Port Triggering

Service Name: AIM

Server IP Address: 192 . 168 . 1 .

	#	Service Name	Start Port	End Port	Server IP Address

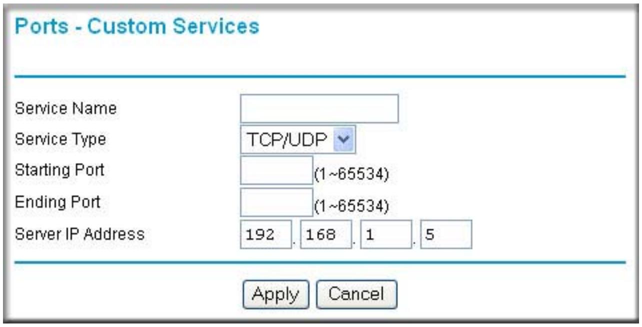
Figure 8-6

2. From the Service Name box, select the service or game that you will host on your network. If the service does not appear in the list, see the following section, Adding a Custom Service.
3. Enter the IP address of the local server in the corresponding Server IP Address box.
4. Click the **Add** button.

Adding a Custom Service

To define a service, game or application that does not appear in the Service Name list, you must determine what port numbers the service will use. For this information, you may need to contact the manufacturer of the program that you wish to use. When you have the port number information, follow these steps:

1. Select **Port Forwarding / Port Triggering** from the Advanced Section of the main menu, as described in the preceding section.
2. Click the **Add Custom Service** button.



Ports - Custom Services

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

Figure 8-7

3. Type the service name in the Service Name box.
4. Type the beginning port number in the Starting Port box.
   - If the application uses only a single port; type the same port number in the Ending Port box.
   - If the application uses a range of ports; type the ending port number of the range in the Ending Port box.
5. Type the IP address of the computer in the Server IP Address box.
6. Click **Apply** to save your changes.

Editing or Deleting a Port Forwarding Entry

To edit or delete a Port Forwarding entry, follow these steps.

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

Local Web and FTP Server Example

If a local computer with a private IP address of 192.168.1.33 acts as a Web and FTP server, configure the Ports menu to forward HTTP (port 80) and FTP (port 21) to local address 192.168.1.33

In order for a remote user to access this server from the Internet, the remote user must know the IP address that has been assigned by your ISP. If this address is 172.16.1.23, for example, an Internet user can access your Web server by directing the browser to http://172.16.1.23. The assigned IP address can be found in the Router Status Menu, where it is shown as the WAN IP Address.

Some considerations for this application are:

- If your account’s IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires.
- If the IP address of the local computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, you can manually configure the computer to use a fixed address.
- Local computers must access the local server using the computers’ local LAN address (192.168.1.33 in this example). Attempts by local computers to access the server using the external IP address (172.16.1.23 in this example) will fail.

Multiple Computers for Internet Gaming

To set up an additional computer to play Age of Empire or Quake III:

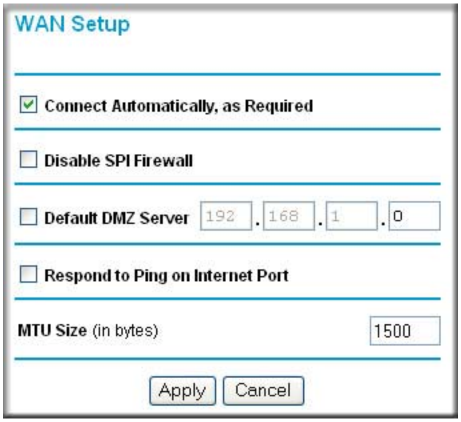
1. Click the button of an unused port in the table.
2. Select the game again from the Services/Games list.
3. Change the beginning port number in the Start Port box.
   For these games, use the supplied number in the default list and add +1 for each additional computer. For example, if you have already configured one computer to play Hexen II (using port 26900), the second computer's port number would be 26901, and the third computer would be 26902.
4. Type the same port number in the End Port box that you typed in the Start Port box.

5. Type the IP address of the additional computer in the Server IP Address box.
6. Click **Apply**.

Some online games and videoconferencing applications are incompatible with NAT. The WPNT834 router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default in the Port Forwarding / Port Triggering Menu. If one local computer acts as a game or videoconferencing host, enter its IP address as the default.

Configuring the WAN Setup Options

The WAN Setup options let you configure a DMZ server, change the MTU size and enable the wireless router to respond to a Ping on the WAN port. These options are discussed below.



WAN Setup

☑ Connect Automatically, as Required

□ Disable SPI Firewall

□ Default DMZ Server 192 . 168 . 1 . 0

□ Respond to Ping on Internet Port

MTU Size (in bytes) 1500

Figure 8-8

Connecting Automatically, as Required

Normally, this option should be checked to enable it. An Internet connection will be made automatically after each timeout, whenever Internet-bound traffic is detected. This provides connection on demand and is potentially cost-saving, in some regions of Europe for example, where Internet services charge by the minute.

If disabled, you must connect manually, using the "Connection Status" button on the Router Status screen. This manual connection will stay up all the time without timeouts.

Disabling the SPI Firewall

The SPI (Stateful Inspection) Firewall protects your LAN against Denial of Service attacks. This should only be disabled in special circumstances.

Setting Up a Default DMZ Server

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

> **Note:** 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 can be used to attack your network.

Incoming traffic from the Internet is normally 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 menu. 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 menu lets you configure a Default DMZ Server.

To assign a computer or server to be a Default DMZ server, follow these steps:

1. Click **WAN Setup** link in the Advanced section of the main menu.
2. Type the IP address for that server. To remove the default DMZ server, replace the IP address numbers with all zeros.
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, click the **Respond to Ping on Internet WAN Port** check box. This should only be used as a diagnostic tool, since it allows your router to be discovered. Do not check this box unless you have a specific reason to do so.

Setting the MTU Size

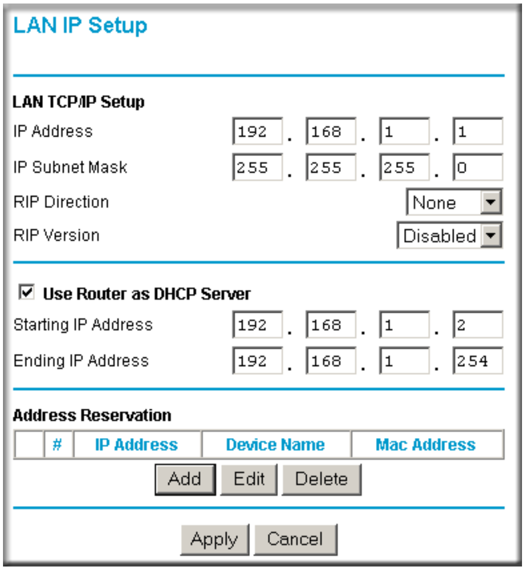
The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, 1492 Bytes for PPPoE connections, or 1436 for PPTP connections. For some ISPs you may need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Any packets sent through the router that are larger than the configured MTU size are repackaged into smaller packets to meet the MTU requirement. To change the MTU size:

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

Using the LAN IP Setup Options

Another category under the Advanced heading is LAN IP Setup. This menu allows configuration of LAN IP services such as DHCP and RIP. From the main menu of the browser interface, under Advanced, click on **LAN IP Setup** to view the LAN IP Setup menu, shown below.



LAN IP Setup

LAN TCP/IP Setup

IP Address 192 . 168 . 1 . 1

IP Subnet Mask 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: Disabled

☑ **Use Router as DHCP Server**

Starting IP Address 192 . 168 . 1 . 2

Ending IP Address 192 . 168 . 1 . 254

Address Reservation

	#	IP Address	Device Name	Mac Address

Figure 8-9

Configuring LAN TCP/IP Setup Parameters

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

- LAN IP address—192.168.1.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-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 menu.

The LAN IP parameters are:

- IP Address
  This is the LAN IP address of the router.
- IP Subnet Mask
  This is 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 (Router Information Protocol) 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 Out Only, the router broadcasts its routing table periodically.
  - When set to Both or In Only, the router incorporates the RIP information that it receives.
  - When set to None, the router does not send any RIP packets and ignores any RIP packets received.
- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.
  - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
  - RIP-2 carries more information. RIP-2B uses subnet broadcasting.

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.

Using the Router as a DHCP server

By default, the router functions as a DHCP (Dynamic Host Configuration Protocol) 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 menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See "Wireless Communications" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.254, although you may 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 menu; otherwise, the router's LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu)

To select another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box. Otherwise, leave it checked.

Using Address Reservation

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

To reserve an IP address:

1. Click the **Add** button.
2. In the IP Address box, type the IP address to assign to the computer or server. (choose an IP address from the router's LAN subnet, such as 192.168.1.x)

3. Type the MAC Address of the computer or server.

> **Tip:** If the computer is already present on your network, you can copy its MAC address from the Attached Devices menu 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**.

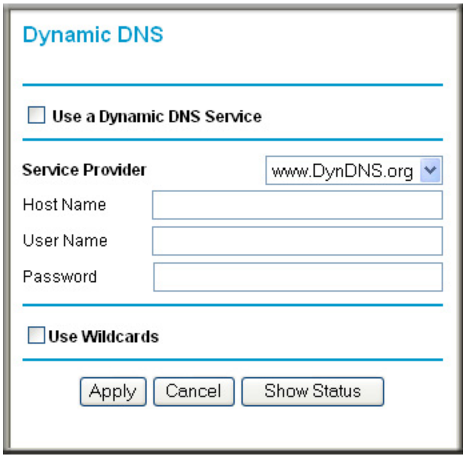
Using a Dynamic DNS Service

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service, which will allow you to register your domain to their IP address, and will forward 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.

The router contains a client that can connect to many popular dynamic DNS services. You can select one of these services and obtain an account with them. Then, whenever your ISP-assigned IP address changes, your router will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

From the main menu of the browser interface, under Advanced, click on **Dynamic DNS**.



Dynamic DNS

☐ Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name:

User Name:

Password:

☐ Use Wildcards

Figure 8-10

To configure Dynamic DNS:

1. Register for an account with one of the dynamic DNS service providers whose names appear in the **Select Service Provider** box. For example, for dyndns.org, go to **www.dyndns.org**.
2. Select the **Use a Dynamic DNS Service** check box.
3. Select the name of your dynamic DNS Service Provider.
4. Type the Host Name (or domain name) that your dynamic DNS service provider gave you.
5. Type the User Name for your dynamic DNS account.
6. Type the Password (or key) for your dynamic DNS account.
7. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the **Use wildcards** check box to activate this feature.
   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
8. Click **Apply** to save your configuration.

Configuring Static Routes

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

From the main menu of the browser interface, under Advanced, click on **Static Routes** to view the Static Routes menu, shown below.

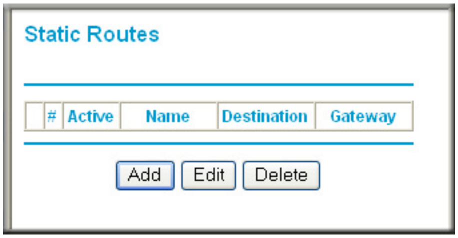
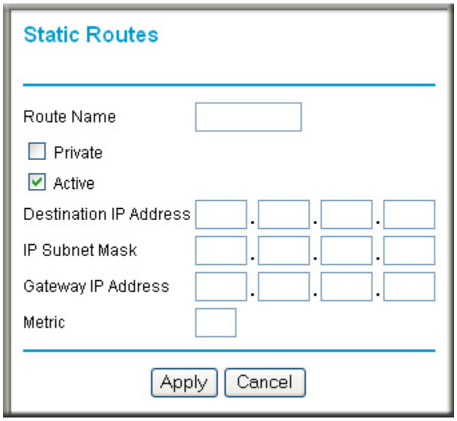


Figure 8-11

To add or edit a Static Route:

1. Click the **Add** button to open the Add/Edit Menu, shown below.



Route Name

☐ Private

☑ Active

Destination IP Address . . .

IP Subnet Mask . . .

Gateway IP Address . . .

Metric

Figure 8-12

2. Type a route name for this static route in the Route Name box.
(This is for identification purposes only.)

3. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Select **Active** to make this route effective.
5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type 255.255.255.255.
7. Type the Gateway IP Address, which must be a router on the same LAN segment as the WPNT834.
8. Type 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.
9. Click **Apply** to have the static route entered into the table.

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 will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

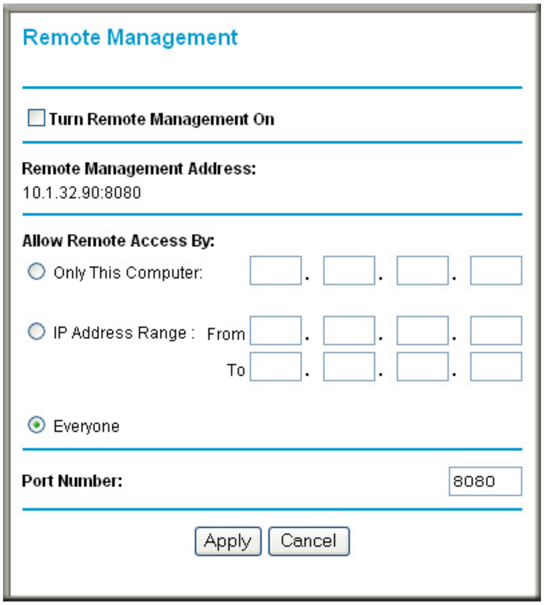
In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. The static route would look like Figure 8-12.

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 fields 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.

Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your WPNT834 router.



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

Figure 8-13

➡	**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 upper and lower case), 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. Specify what external 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.

  a. To allow access from any IP address on the Internet, select **Everyone**.

  b. To allow access from a range of IP addresses on the Internet, select **IP address range**. Enter a beginning and ending IP address to define the allowed range.

  c. To allow access from a single IP address on the Internet, select **Only this computer**. Enter the IP address that will be allowed access.

3. Specify the Port Number for accessing the management interface.

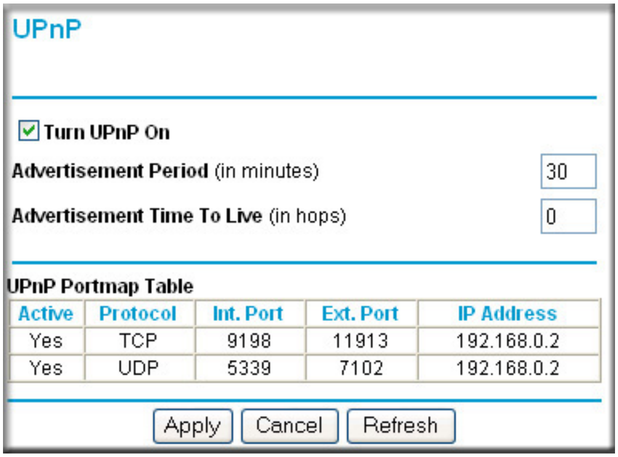
Web browser access normally uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote management Web interface. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate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

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

➡	**Note:** When accessing your router from the Internet, type your router's WAN IP address into your browser's Address (in Internet Explorer) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, then enter http://134.177.0.123:8080 in your browser.

Using Universal Plug and Play (UPnP)

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



UPnP

☑ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time To Live (in hops) 0

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
Yes	TCP	9198	11913	192.168.0.2
Yes	UDP	5339	7102	192.168.0.2

Figure 8-14

From the main menu of the browser interface, under Advanced, click on **UPnP**. Set up UPnP according to the guidelines below.

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

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

Advertisement Period—the Advertisement Period is how often the router will broadcast 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 may 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 may be necessary to increase this value a little.

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