RangeMax Dual Band Wireless-N Modem Router DGND3300 User Manual

NETGEAR

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134 USA

202-10463-02
September 2009
v1.0

Product Registration, Support, and Documentation

Register your product at *http://www.NETGEAR.com/register*. Registration is required before you can use our telephone support service. Product updates and Web support are always available by going to: *http://www.netgear.com/support*.

Setup documentation is available on the CD, on the support website, and on the documentation website. When the wireless router is connected to the Internet, click the Knowledgebase or the Documentation link under Web Support in the main menu to view support information.

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks, and RangeMax and Smart Wizard are trademarks of NETGEAR. Inc. in the United States and/or other countries. Microsoft, Windows, and Windows NT are registered trademarks and Windows Vista is a trademark of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving 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.

Certificate of the Manufacturer/Importer

It is hereby certified that the RangeMax Dual Band Wireless-N Modem Router has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das RangeMax Dual Band Wireless-N Modem Router gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

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.

Europe – EU Declaration of Conformity

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

EN300 328, EN301 893, EN301 489-17, EN60950

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the DGND3300 product package.

Europe – Declaration of Conformity 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, _e Radiolan spĺňa základné po_iadavky 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.

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., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model DGND3300 RangeMax Dual Band Wireless-N Modem Router complies with Part 15 of FCC 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.

RangeMax Dual Band Wireless-N Modem Router

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user's right to operate the equipment.

Maximum Wireless Signal Rate Derived from IEEE Standard 802.11 Specifications

Actual data 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.

Product and Publication Details

Model Number:	DGND3300
Publication Date:	September 2009
Product Family:	Modem Router
Product Name:	RangeMax Dual Band Wireless-N Modem Router
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10463-02

Contents

About This Manual

Chapter 1
Configuring Your Internet Connection

Chapter 2
Safeguarding Your Network

Chapter 6
Customizing Your Network Settings

Chapter 7
Fine-Tuning Your Network

Chapter 8
Troubleshooting

Appendix A
Default Configuration and Technical Specifications

Appendix B
Related Documents

Index

About This Manual

The user manual provides information for configuring the features of the NETGEAR® RangeMax Dual Band Wireless-N Modem Router beyond initial configuration settings. Initial configuration instructions can be found in the *Setup Manual*. You should have basic to intermediate computer and Internet skills.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical conventions**. This manual uses the following typographical conventions:

Italic	Emphasis, books, CDs
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
Italic	URL links

- **Formats**. This manual uses the following formats to highlight special messages:

➡	**Note:** This format is used to highlight information of importance or special interest.

💡	**Tip:** This format is used to highlight a procedure that will save time or resources.

⚠	**Warning:** Ignoring this type of note might result in a malfunction or damage to the equipment, a breach of security, or a loss of data.

- **Scope**. This manual is written for the Dual Band Wireless-N Modem Router according to these specifications:

Product Version	RangeMax Dual Band Wireless-N Modem Router
Manual Publication Date	September 2009

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, "Related Documents."

Note: Product updates are available on the NETGEAR, Inc. website at *http://www.netgear.com/support.*

How to Print This Manual

To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

NETGEAR, Inc. is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the Dual Band Wireless-N Modem Router was introduced.

Part Number	Version Number	Date	Description
202-10463-02	1.0	September 2009	USB features added.
202-10463-01	1.0	March 2009	Original publication.

Chapter 1
Configuring Your Internet Connection

This chapter describes how to configure your Dual Band Wireless-N Modem Router Internet connection. When you install your modem router using the *Resource CD* as described in the *Setup Manual*, these settings are configured automatically for you. This chapter provides instructions on how to log in to the modem router for further configuration.

➡	**Note:** NETGEAR recommends that Windows OS users use the Smart Wizard™ on the *Resource CD* for initial configuration. Mac and Linux OS users should access the *Setup Manual* on the *Resource CD*.

This chapter includes:

- "Using the Setup Manual"
- "Logging In to Your Modem Router" on page 1-2
- "Using the Setup Wizard" on page 1-3
- "Viewing or Manually Configuring Your ISP Settings" on page 1-4
- "Configuring ADSL Settings" on page 1-8

Using the Setup Manual

For first-time installation of your wireless modem router, refer to the *Setup Manual*. The Setup Manual explains how to launch the NETGEAR Smart Wizard on the *Resource CD* to step you through the procedure to connect your modem router and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network. After initial configuration using the Setup Manual, you can use the information in this Reference Manual to configure additional features of your wireless modem router.

For installation instructions in a language other than English, see the language options on the *Resource CD*.

Logging In to Your Modem Router

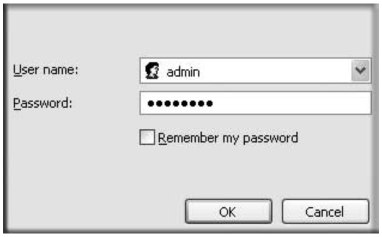
You can log in to the modem router to view or change its settings. Links to Knowledge Base and documentation are also available on the modem router main menu.

➡	**Note:** Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document in "Preparing Your Network" in Appendix B.

When you have logged in, if you do not click **Logout**, the modem router waits for 5 minutes after no activity before it automatically logs you out.

To log in to the modem router:

1. Type **http://www./routerlogin.net**, or **http://www.routerlogin.com,** or the modem router's LAN IP address (default is 192.168.0.1) in the address field of your browser, and then press Enter. A login window displays:



User name: admin

Password: ••••••••

□ Remember my password

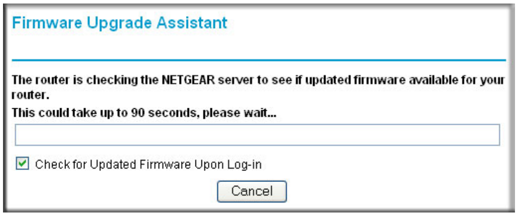
Figure 1-1

2. Enter **admin:**for the modem router user name and your password (or the default, **password**). For information about how to change the password, see "Changing the Built-In Password" on page 3-2.

➡	**Note:** The modem 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.

If the modem router has never been configured, the Smart Wizard screen displays. After the modem router has been configured, the Firmware Upgrade assistant will appear.

- **Checking for Firmware Updates screen**. After initial configuration, this screen displays unless you previously cleared the **Check for Updated Firmware Upon Log-in** check box.



Firmware Upgrade Assistant

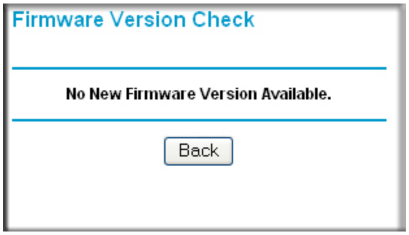
The router is checking the NETGEAR server to see if updated firmware available for your router.
This could take up to 90 seconds, please wait...

☑ Check for Updated Firmware Upon Log-in

Figure 1-2

➡	**Note:** If the modem router is not configured (is in its factory default state) when you log in, the Setup Wizard displays. See "Using the Setup Wizard" on page 1-4.

If the modem router discovers a newer version of the firmware, you are asked if you want to upgrade to the new firmware (see "Upgrading the Firmware" on page 4-1 for details). If no new firmware is available, the following message displays.



Firmware Version Check

No New Firmware Version Available.

Figure 1-3

- **Router Status screen**. The Router Status screen displays if the modem router has not been configured yet or has been reset to its factory default settings. See "Viewing Modem Router Status Information" on page 4-4.

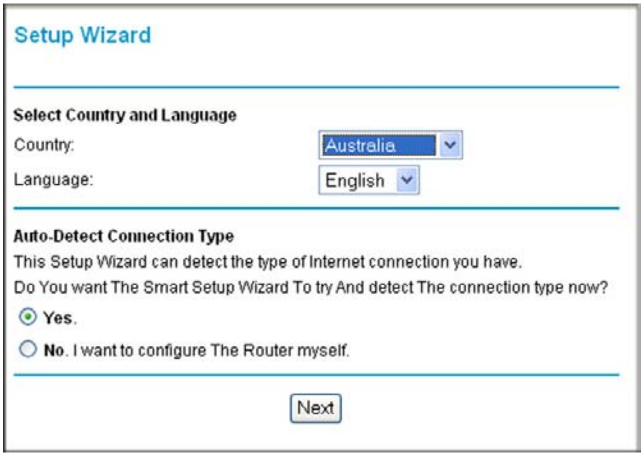
  You can use the Setup Wizard to automatically detect your Internet connection as described in "Using the Setup Wizard" on page 1-3, or you can bypass the Setup Wizard and manually configure your Internet connection as described in "Viewing or Manually Configuring Your ISP Settings" on page 1-4.

Using the Setup Wizard

You can manually configure your Internet connection using the Basic Settings screen, or you can allow the Setup Wizard to detect your Internet connection. The Setup Wizard searches 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.

To use the Setup Wizard:

1. To go to the Setup Wizard screen, from the top of the main menu, select **Setup Wizard**.



Setup Wizard

Select Country and Language

Country: Australia

Language: English

Auto-Detect Connection Type

This Setup Wizard can detect the type of Internet connection you have.

Do You want The Smart Setup Wizard To try And detect The connection type now?

● Yes.

○ No. I want to configure The Router myself.

Figure 1-4

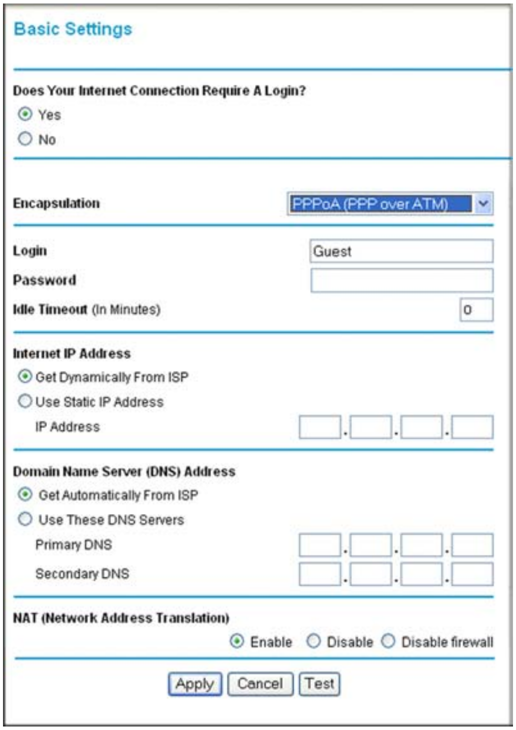
2. Select **Yes** for the Auto-Detect Connection Type, and then click **Next** to proceed.
3. Enter your ISP settings, as needed.
4. At the end of the Setup Wizard, click **Test** to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 8, “Troubleshooting.”

Viewing or Manually Configuring Your ISP Settings

To view or configure the basic settings:

1. Log in to the modem router as described in “Logging In to Your Modem Router” on page 1-2.

2. Select Basic Settings from the modem router menu to display the Basic Settings screen:



Basic Settings

Does Your Internet Connection Require A Login?

● Yes

○ No

Encapsulation: PPPoA (PPP over ATM)

Login: Guest

Password:

Idle Timeout (In Minutes): 0

Internet IP Address

● Get Dynamically From ISP

○ Use Static IP Address

IP Address: . . .

Domain Name Server (DNS) Address

● Get Automatically From ISP

○ Use These DNS Servers

Primary DNS: . . .

Secondary DNS: . . .

NAT (Network Address Translation)

● Enable ○ Disable ○ Disable firewall

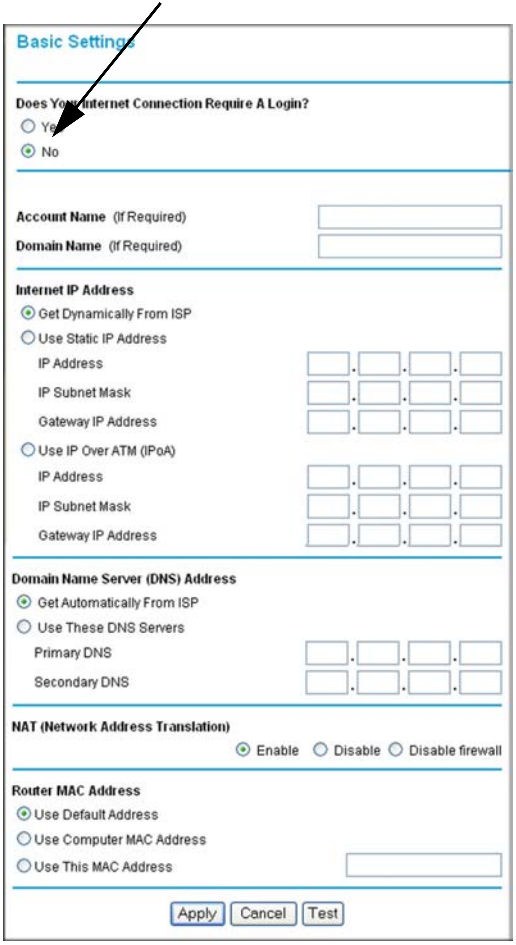
Figure 1-5

3. 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 the encapsulation method. Enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. If your ISP does not require a login, enter the account name, if required, and the domain name, if required.
4. 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.
5. If no login is required, you can specify the MAC Address setting.
6. Click **Apply** to save your settings.
7. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to.

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 modem router automatically logs you in

The fields that are displayed depend on whether or not your Internet connection requires a login.

ISP *does not* require login



Basic Settings

Does Your Internet Connection Require A Login?
○ Yes
● No

Account Name (If Required) [ ]
Domain Name (If Required) [ ]

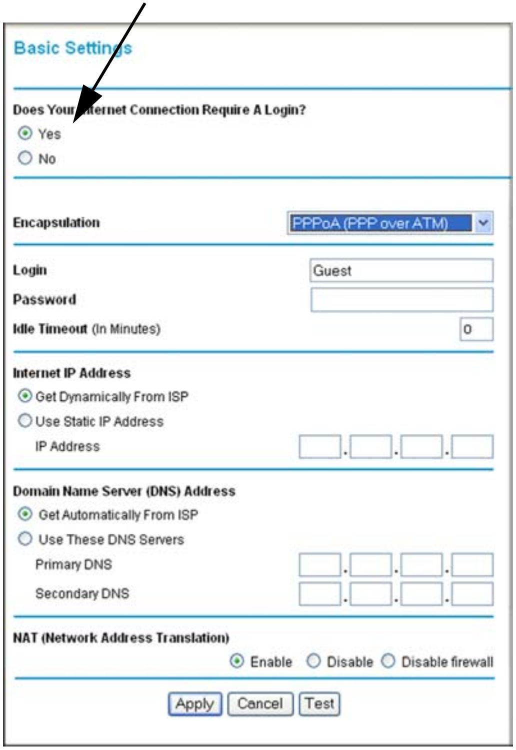
Internet IP Address
● Get Dynamically From ISP
○ Use Static IP Address
IP Address [ ].[ ].[ ].[ ]
IP Subnet Mask [ ].[ ].[ ].[ ]
Gateway IP Address [ ].[ ].[ ].[ ]
○ Use IP Over ATM (IPoA)
IP Address [ ].[ ].[ ].[ ]
IP Subnet Mask [ ].[ ].[ ].[ ]
Gateway IP Address [ ].[ ].[ ].[ ]

Domain Name Server (DNS) Address
● Get Automatically From ISP
○ Use These DNS Servers
Primary DNS [ ].[ ].[ ].[ ]
Secondary DNS [ ].[ ].[ ].[ ]

NAT (Network Address Translation)
● Enable ○ Disable ○ Disable firewall

Router MAC Address
● Use Default Address
○ Use Computer MAC Address
○ Use This MAC Address [ ]

ISP *does* require login



Basic Settings

Does Your Internet Connection Require A Login?
● Yes
○ No

Encapsulation: PPPoA (PPP over ATM)

Login: Guest
Password [ ]
Idle Timeout (In Minutes): 0

Internet IP Address
● Get Dynamically From ISP
○ Use Static IP Address
IP Address [ ].[ ].[ ].[ ]

Domain Name Server (DNS) Address
● Get Automatically From ISP
○ Use These DNS Servers
Primary DNS [ ].[ ].[ ].[ ]
Secondary DNS [ ].[ ].[ ].[ ]

NAT (Network Address Translation)
● Enable ○ Disable ○ Disable firewall

Figure 1-6

The following table explains the fields in the Basic Settings screen.

Table 1-1. 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.	Login	The login name provided by your ISP. This is often an e-mail address.
	Password	The password that you use to log ISP.
	Service Name	If your ISP provided a Service Name, enter it here.
	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 modem 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 modem router to which your modem router will connect. • **Use IP Over ATM (PoA)**. This option is only available if your ISP does not require a log in.
Domain Name Server (DNS) Address		The DNS server is used to look up site addresses based on their names. • **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address. • **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Table 1-1. Basic Settings screen fields (continued)

Settings		Description
NAT (Net Address Translation)		NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices. • **Enable**. Usually NAT is enabled. • **Disable**. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure that you do not require it. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses that the modem router uses. Classical routing should be selected only by experienced users[a] • **Disable firewall**. This disables the firewall in addition to disabling NAT. With the firewall disabled, the protections usually provided to your network are disabled.
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 modem 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.

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

Configuring ADSL Settings

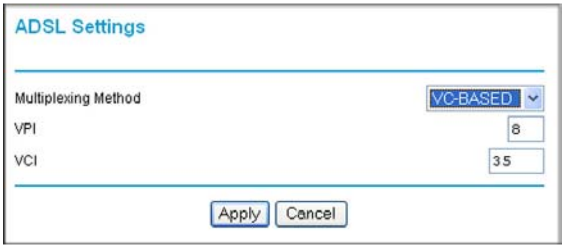
Note: For information about how to install ADSL filters, see the *Setup Manual*.

NETGEAR recommends that you use the Setup Wizard to automatically detect and configure your ADSL settings. This usually works fine. However, if you have technical experience and are sure of the multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI), you can specify those settings here.

➡	**Note:** NETGEAR recomments using the Setup Wizard to select the correct country to optimize detection of the ADSL settings.

If your ISP provided you with a multiplexing method or VPI/VCI number, then enter the setting:

1. From the main menu, select ADSL Settings.The ADSL Settings screen displays.



ADSL Settings

Multiplexing Method: VC-BASED

VPI: 8

VCI: 35

Figure 1-7

2. In the **Multiplexing Method** drop-down list, select **LLC-based** or **VC-based**.
3. For the VPI, type a number between 0 and 255. The default is 8.
4. For the VCI, type a number between 32 and 65535. The default is 35.
5. Click **Apply**.

Chapter 2
Safeguarding Your Network

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

⚠	**Warning:** Computers can connect wirelessly at a range of several hundred feet. This can allow others outside of your immediate area to access your network.

This chapter includes:

- "Planning Your Wireless Network
- "Manually Configuring Your Wireless Settings" on page 2-4
- "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10
- "Connecting Additional Wireless Client Devices After WPS Setup" on page 2-14
- "Restricting Access to Your Modem Router" on page 2-16
- "Wireless Guest Networks" on page 2-17

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 11N SSID for the modem router is **NETGEAR-DualBand-N**. The default 11G SSID is **NETGEAR-2.4-G**.
  - The wireless mode (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 2-4.

- Push 'N' Connect (WPS) automatically implements wireless security on the modem router while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). You activate WPS by pressing a WPS button on the modem router, clicking an onscreen WPS button, or entering a PIN number. This generates a new SSID and implements WPA/WPA2 security.

  > **Note:** NETGEAR’s Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see *http://www.wi-fi.org*). All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.

  To set up your wireless network using the WPS feature:

  - Use the modem router dome, which works as a WPS button (there is also an onscreen WPS button), or enter the PIN of the wireless device.
  - Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA2 capable, and that they support WPS configuration.

  See “Using Push 'N' Connect (WPS) to Configure Your Wireless Network” on page 2-10.

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the modem 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 modem 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).

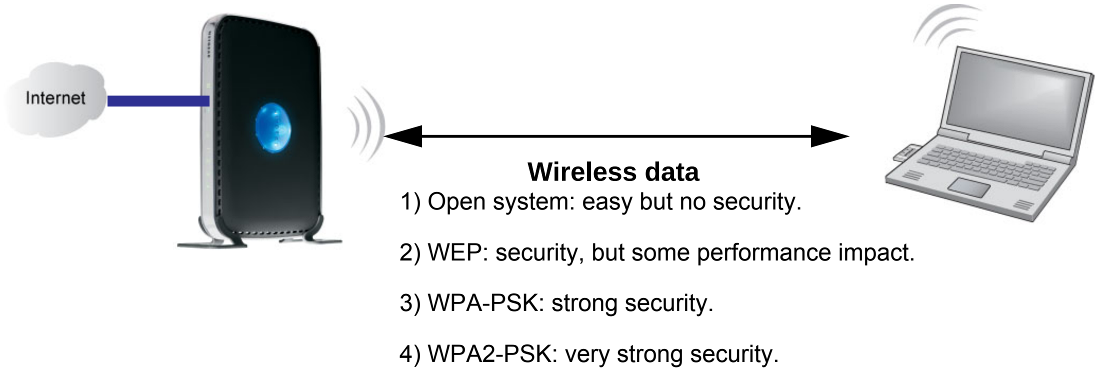
The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

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 Dual Band Wireless-N Modem Router 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:



Wireless data

1) Open system: easy but no security.

2) WEP: security, but some performance impact.

3) WPA-PSK: strong security.

4) WPA2-PSK: very strong security.

Figure 2-1

- **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, see the link to the online document in "Wireless Networking Basics" in Appendix B.

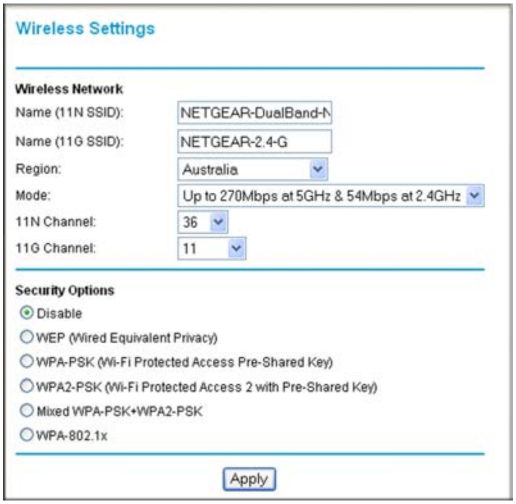
Manually Configuring Your Wireless Settings

You can view or manually configure the wireless settings for the modem router in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first.

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

To view or manually configure the wireless settings:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the modem router.
2. Select **Wireless Settings** from the main menu to display the Wireless Settings screen:



Wireless Settings

Wireless Network

Name (11N SSID):	NETGEAR-DualBand-N
Name (11G SSID):	NETGEAR-2.4-G
Region:	Australia
Mode:	Up to 270Mbps at 5GHz & 54Mbps at 2.4GHz
11N Channel:	36
11G Channel:	11

Security Options

● Disable
○ WEP (Wired Equivalent Privacy)
○ WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)
○ WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key)
○ Mixed WPA-PSK+WPA2-PSK
○ WPA-802.1x

Figure 2-2

The settings for this screen are explained in Table 2-1 on page 2-5.

3. Select the region in which the modem 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.

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

Table 2-1. Wireless Settings

Settings	Description
Name (11N SSID) Name (11G SSID)	This is the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device that you want to participate in a wireless network must use the SSID.
Region	The location where the router is used.
Mode	Specify which 802.11 data communications protocol is used. You can select one of the following modes: • **Up to 270 Mbps at 2.4 GHz**. Performance mode, using channel expansion to achieve the 270 Mbps data rate. The Dual Band Wireless-N Modem Router uses the channel you selected as the primary channel and expands to the secondary channel (primary channel +4 or –4) to achieve a 40 MHz frame-by-frame bandwidth. The Dual Band Wireless-N Modem Router detects channel usage and disables frame-by-frame expansion if the expansion would result in interference with the data transmission of other access points or clients. • **Up to 270 Mbps at 5 GHz and 54 Mbps at 2.4 GHz**. This is the default mode, which is recommended. • **Up to 130 Mbps at 2.4 GHz**. Neighbor friendly mode, for reduced interference with neighboring wireless networks. Provides two transmission streams with different data on the same channel at the same time, but also allows 802.11b and 802.11g wireless devices. • **Up to 130 Mbps at 5 GHz and 54 Mbps at 2.4 GHz**. Legacy mode, for compatibility with the slower 802.11b and 802.11g wireless devices.
11 N Channel 11 G Channel	The wireless channel fields determine the operating frequency used for the 11N or 11G wireless networks. Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best.

Table 2-1. Wireless Settings (continued)

Settings	Description
Security Options	• **Disable**. You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security. • **WEP (Wired Equivalent Privacy)**. Use encryption keys and data encryption for data security. Select 64-bit or 128-bit encryption. See “Configuring WEP Wireless Security. • **WPA-PSK (WiFi Protected Access Pre-Shared Key).** Allow only computers configured with WPA to connect to the modem router. • **WPA2-PSK Wi-Fi Protected Access with 2 Pre-Shared Keys)**. Allow only computers configured with WPA2 to connect to the modem router. • **Mixed WPA-PSK + WPA2-PSK**. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the modem router. • **WPA-802.1x**. • For WPA or WPA2 configuration, see “Configuring WPA, WPA2, or Mixed WPA2 + WPA Wireless Security” on page 2-8.
WPA2-PSK Security Encryption	**Network Key (8-63 characters)**.

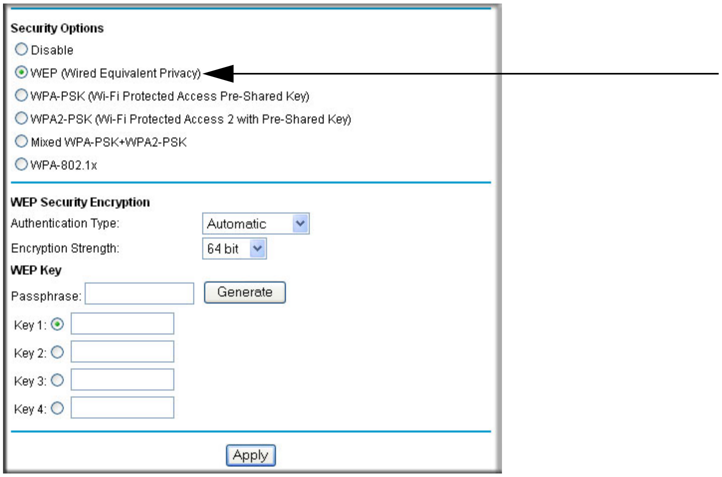
Configuring WEP Wireless Security

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 modem router from a wired computer to make further changes.

To configure WEP data encryption:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the modem router.
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:



Security Options

○ Disable

● WEP (Wired Equivalent Privacy)

○ WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)

○ WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key)

○ Mixed WPA-PSK+WPA2-PSK

○ WPA-802.1x

WEP Security Encryption

Authentication Type: Automatic

Encryption Strength: 64 bit

WEP Key

Passphrase: ______ Generate

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Apply

Figure 2-3

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

➡	**Note:** The authentication scheme is separate from the data encryption. You can select an authentication scheme that requires a shared key but still leaves the data transmissions unencrypted. If you require strong security, 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 modem 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 Mixed WPA2 + WPA Wireless Security

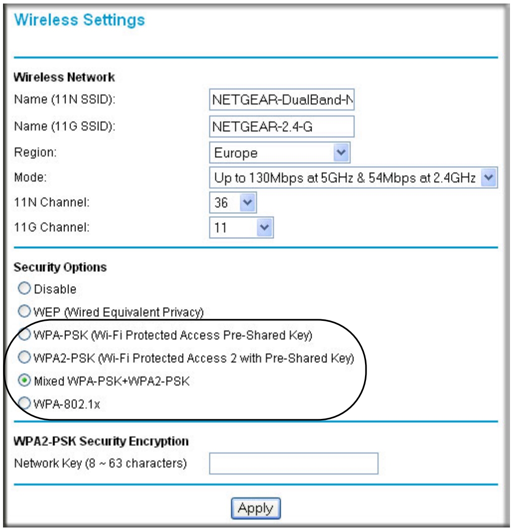
To set up wireless security, you can either manually configure it in the Wireless Settings screen, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security (see “Using Push 'N' Connect (WPS) to Configure Your Wireless Network” on page 2-10.) WPA2 is the strongest security setting and is recommended if the client supports it.

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 modem router from a wired computer to make further changes.

To configure WPA or WPA2 in the modem router:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the modem router.
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.



Wireless Settings

Wireless Network

Name (11N SSID): NETGEAR-DualBand-N

Name (11G SSID): NETGEAR-2.4-G

Region: Europe

Mode: Up to 130Mbps at 5GHz & 54Mbps at 2.4GHz

11N Channel: 36

11G Channel: 11

Security Options

○ Disable

○ WEP (Wired Equivalent Privacy)

○ WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)

○ WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key)

● Mixed WPA-PSK+WPA2-PSK

○ WPA-802.1x

WPA2-PSK Security Encryption

Network Key (8 ~ 63 characters)

Figure 2-4

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. If prompted, enter the settings for the Radius server. For WPA-802.1x or WPA2-802.1x, these settings are required for communication with the primary Radius server.

Note: Radius server only applies to WPA-802.1x, and not to Mixed WPA + WPA2.

- **Primary Radius Server IP Address**. The IP address of the Radius server. The default is 0.0.0.0
- **Radius Port**. Port number of the Radius server. The default is 1812.

- **Shared Key**. This is shared between the wireless access point and the Radius server during authentication.

7. To save your settings, click **Apply**.

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

If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the modem router's SSID and security settings and, at the same time, connect the wireless client securely and easily to the modem router. Look for the symbol on your client device (computers that will connect wirelessly to the modem router are clients). WPS automatically configures the network name (SSID) and wireless security settings for the modem router (if the modem router is in its default state) and broadcasts these settings to the wireless client.

Note: NETGEAR's Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see *http://www.wi-fi.org*). All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.

Some considerations regarding WPS are:

- WPS supports only WPA-PSK and WPA2-PSK wireless security. WEP security is not supported by WPS.
- 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 additional WPS capable devices. See "Adding Both WPS and Non-WPS Clients" on page 2-15.

A WPS client can be added using the Push Button method or the PIN method.

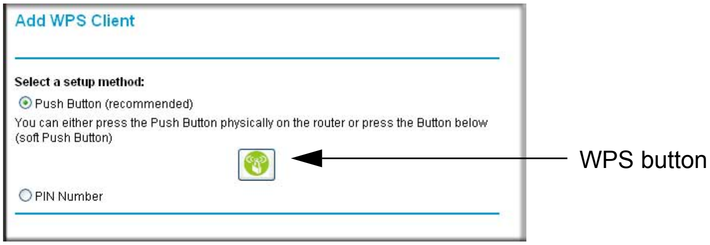
- **Using the Push Button**. This is the preferred method. See the following section, "Using a WPS Button to Add a WPS Client.
- **Entering a PIN**. For information about using the PIN method, see "Using PIN Entry to Add a WPS Client" on page 2-12.

Using a WPS Button to Add a WPS Client

Any wireless computer or wireless adapter that will connect to the modem 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 modem router WPS button to add a WPS client:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. On the modem router main menu, select Add a WPS Client, and then click **Next**. The following screen displays:



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

Figure 2-5

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

3. Either press the modem router dome for a few seconds, which works as a WPS button, or click the onscreen button.

   The modem router tries to communicate with the client 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 modem router screen to check for a message.

   The modem router WPS screen displays a message confirming that the client was added to the wireless network. The modem router generates an SSID, and implements WPA/WPA2 wireless security. The modem router will keep these wireless settings unless you change them, or you clear the **Keep Existing Wireless Settings** check box in the Advanced Wireless Settings screen. See "Restricting Access to Your Modem Router" on page 2-16

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 2-4.

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

Note: If no WPS-capable client devices are located during the 2-minute time frame, the SSID will not be changed, and no security will be implemented on the modem router.

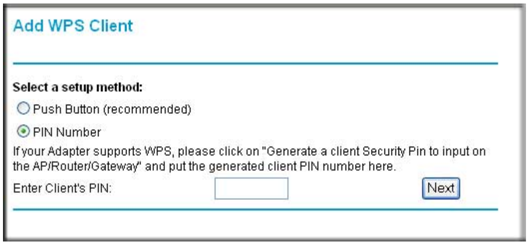
Using PIN Entry to Add a WPS Client

Any wireless computer or wireless adapter that will connect to the modem 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 modem router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the modem router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

To use a PIN to add a WPS client:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. On the modem router main menu, select Add a WPS Client (computers that will connect wirelessly to the modem router are clients), and then click **Next**. The Add WPS Client screen displays:



Add WPS Client

Select a setup method:

○ Push Button (recommended)

● PIN Number

If your Adapter supports WPS, please click on "Generate a client Security Pin to input on the AP/Router/Gateway" and put the generated client PIN number here.

Enter Client's PIN:

Figure 2-6

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

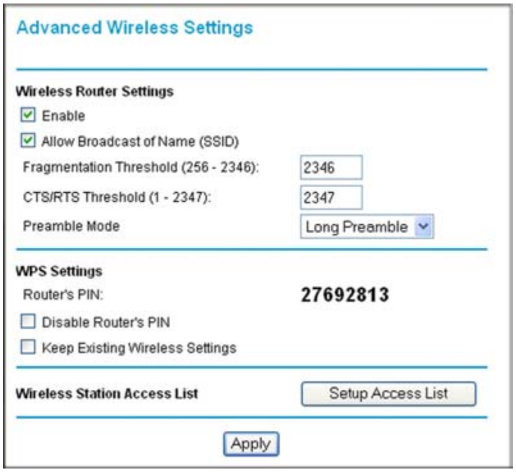
4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility’s instructions to generate a PIN. Take note of the client PIN.
5. From the modem router Add WPS Client screen, enter the client PIN number, and then click **Next**.
   - The modem router tries to communicate with the client for 4 minutes.
   - The modem router WPS screen displays a message confirming that the client was added to the wireless network. The modem router generates an SSID, and implements WPA/WPA2 wireless security.
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 2-4

To access the Internet from any computer connected to your modem router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the modem router’s Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute time frame, the SSID will not be changed and no security will be implemented on the modem router.

Configuring Advanced WPS Settings

From the main menu, select Advanced Wireless Settings to display the following screen:



Advanced Wireless Settings

Wireless Router Settings

☑ Enable

☑ Allow Broadcast of Name (SSID)

Fragmentation Threshold (256 - 2346): 2346

CTS/RTS Threshold (1 - 2347): 2347

Preamble Mode: Long Preamble

WPS Settings

Router's PIN: 27692813

☐ Disable Router's PIN

☐ Keep Existing Wireless Settings

Wireless Station Access List

Figure 2-7

The WPS settings show the modem router PIN, **Disable Router's PIN**, and the **Keep Existing Wireless Settings** check box.

By default, the **Keep Existing Wireless Settings** check box is cleared. This allows the modem router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the modem router automatically selects this check box so that your SSID and wireless security settings remain the same if you add WPS-enabled devices or if you manually add non WPS-capable devices later.

Note: If you clear the **Keep Existing Wireless Settings** check box, all wireless settings and connections will be lost if a WPS client is added.

Connecting Additional Wireless Client Devices After WPS Setup

You can add more WPS clients to your wireless network, or you can add a combination of WPS-enabled clients and clients without WPS.

Adding More WPS Clients

Note: Your wireless settings remain the same when you add another WPS-enabled client, as long as the **Keep Existing Wireless Settings** check box is selected in the Advanced Wireless screen (listed under the Advanced heading in the modem router main menu). If you clear this check box, when you add the client, a new SSID and passphrase will be generated, and all existing connected wireless clients will be disassociated and disconnected from the modem router.

To add a wireless client device that is WPS-enabled:

1. Follow the procedures in "Using a WPS Button to Add a WPS Client" on page 2-11 or "Using PIN Entry to Add a WPS Client" on page 2-12.
2. To view a list of all devices connected to your modem router (including wireless and Ethernet-connected), see "Viewing a List of Attached Devices" on page 4-8.

Adding Both WPS and Non-WPS Clients

For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see "Manually Configuring Your Wireless Settings" on page 2-4).

To connect a combination of non-WPS enabled and WPS-Enabled clients to the modem router:

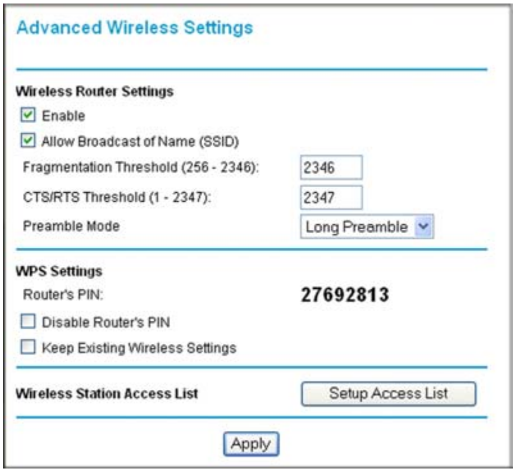
1. Configure the network names (SSIDs), select the WPA/PSK + WPA2/PSK radio button on the Wireless Settings screen (see "Manually Configuring Your Wireless Settings" on page 2-4). and click **Apply**.
2. On the WPA/PSK + WPA2/PSK screen, select a passphrase and click **Apply**. Record this information to add additional clients.
3. For the non-WPS devices that you want to connect, open the networking utility and follow the utility's instructions to enter the SSID, WPA/PSK + WPA2/PSK security method, and passphrase.
4. For the WPS devices that you want to connect, follow the procedure "Using a WPS Button to Add a WPS Client" on page 2-11 or "Using PIN Entry to Add a WPS Client" on page 2-12.

   > ➡ **Note:** To make sure that your new wireless settings remain in effect, verify that the **Keep Existing Wireless Settings** checkbox is selected in the WPS Settings screen.

5. To view a list of all devices connected to your modem router (including wireless and Ethernet-connected), see "Viewing a List of Attached Devices" on page 4-8.

Restricting Access to Your Modem Router

You can use the Advanced Wireless Settings screen to enable or disable the wireless router radio and the SSID broadcast. From the main menu, select **Advanced Wireless Settings** to display the following screen:



Advanced Wireless Settings

Wireless Router Settings

☑ Enable

☑ Allow Broadcast of Name (SSID)

Fragmentation Threshold (256 - 2346): 2346

CTS/RTS Threshold (1 - 2347): 2347

Preamble Mode: Long Preamble

WPS Settings

Router's PIN: **27692813**

□ Disable Router's PIN

□ Keep Existing Wireless Settings

Wireless Station Access List

Figure 2-8

- **Enable Wireless Router Radio**.
  You can completely turn off the wireless portion of the modem router. For example, if you use your notebook computer to wirelessly connect to your modem router, and you take a business trip, you can turn off the wireless portion of the modem router while you are traveling. Other members of your household who use computers connected to the modem router via Ethernet cables can still use the modem router. To do this, clear the **Enable Wireless Access Point** check box on the Advanced Wireless Settings screen, and then click **Apply**.
- **Enable SSID Broadcast**. Clear this check box to disable broadcast of the SSID, so that only devices that know the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP.

> **Note:** The SSID of any wireless access adapters must match the SSID you configure in the modem router. If they do not match, you will not get a wireless connection to the modem router.

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

- **WPS Settings**. These are Push 'N' connect settings used by the modem router when WPS clients are added.
  - **Router's PIN**. The number that the modem router broadcasts when adding a WPS client with the PIN method.
  - **Disable Router PIN**. Selecting this checkbox disables the modem router's PIN.
  - **Keep Existing Wireless Settings**. This checkbox is cleared by default so that the modem router network name (SSID) and security can be set automatically if Push 'N' Connect (WPS) is used to set up the network. When the first WPS client is added, this checkbox is automatically selected so that the SSID and security remain the same when additional clients are added.

  For information about adding WPS clients, see "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10.
- **Restricting access by MAC address**. You can use a Wireless Card Access List to restrict access. See "Restricting Access by MAC Address" on page 3-2.

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.

The Guest Network Settings screen that you see depends on the setting in the **Wireless Mode** field on the Wireless Settings screen and on which selection you make from the main menu. The Guest Network selection is grayed out if it is not available. The following table shows wireless modes, menu selections, and guest networks.

Table 2-2. Wireless Modes and Guest Networks

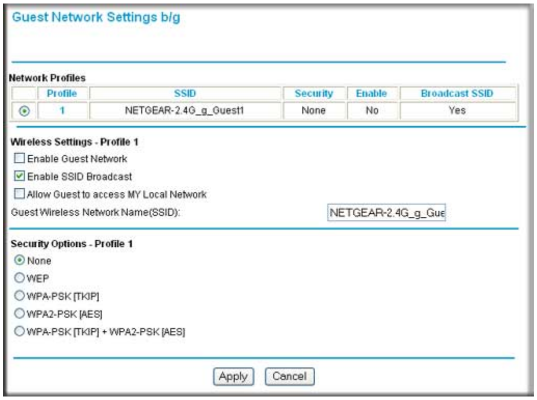
Mode in Wireless Settings Screen	Menu Selection	Guest Network Default SSID	Wireless Compatibility
Up to 270Mbps at 5GHz & 54Mbps at 2.4GH (factory default setting)	Guest Network a/n	NETGEAR-5G_a_n_Guest1	• 5GHz 802.11a • 5GHz 802.11n
	Guest Network b/g	NETGEAR-2.4G_g_Guest1	• 2.4GHz 802.11g • 2.4GHz 802.11b
Up to 270Mpbs	Guest Network b/g/n	NETGEAR-2.4G_n_Guest1	• 2.4GHz 802.11n • 2.4GHz 802.11g • 2.4GHz 802.11b

Table 2-2. Wireless Modes and Guest Networks (continued)

Mode in Wireless Settings Screen	Menu Selection	Guest Network Default SSID	Wireless Compatibility
Up to 130Mbps at 5GHz & 54Mbps at 2.4GHz	Guest Network a/n	NETGEAR-2.4G_n_Guest1	• 5GHz 802.11a • 5GHz 802.11n
	Guest Network b/g	NETGEAR-2.4G_g_Guest1	• 2.4GHz 802.11g • 2.4GHz 802.11b
Up to 130 Mbps at 2.4GHz	Guest Network a/n	NETGEAR-2.4G_n_Guest1	• 2.4GHz 802.11n • 2.4GHz 802.11g • 2.4GHz 802.11b

To configure a wireless guest network:

1. In the main menu, under Setup, select either Wireless Guest Network g/b or Wireless Guest Network a, n. A Wireless Guest Network Settings screen similar to the following figure displays:



Guest Network Settings b/g

Network Profiles

	Profile	SSID	Security	Enable	Broadcast SSID
●	1	NETGEAR-2.4G_g_Guest1	None	No	Yes

Wireless Settings - Profile 1

☐ Enable Guest Network
☑ Enable SSID Broadcast
☐ Allow Guest to access MY Local Network

Guest Wireless Network Name(SSID): NETGEAR-2.4G_g_Gue

Security Options - Profile 1

● None
○ WEP
○ WPA-PSK [TKIP]
○ WPA2-PSK [AES]
○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Figure 2-9

2. Make sure that the **Enable Guest Network** check box is selected.

3. You can specify whether the SSID broadcast is enabled, and whether you want to allow the guest to access your local network. You can also change the **Guest Wireless Network Name (SSID)**, enter a name in the field.

> **Note:** NETGEAR strongly recommends that you change the default guest network name (SSID) from the default name to a different name. Note that the name is case-sensitive. For example, GuestNetwork is not the same as Guestnetwork.

4. Enter a value of up to 32 alphanumeric characters. For the selected guest network, the same name must be assigned to all wireless devices in your network.

➡	**Note:** Wireless security is disabled by default. NETGEAR strongly recommends that you implement wireless security for the guest network.

5. To configure wireless security for the guest network, enter the security options. This process is very similar to configuring wireless security for the modem router. For more information, see "Configuring WEP Wireless Security" on page 2-6 and "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10.

6. When you have finished making changes, click **Apply**.

Chapter 3
Protecting Your Network

This chapter describes how to use the content filtering and reporting features of the Dual Band Wireless-N Modem Router to protect your network.

This chapter includes the following sections:

> **Note:** For information about restricting access to USB storage devices, see “Configuring USB Storage Advanced Settings” on page 5-8.

Protecting Access to Your Modem Router

For security reasons, the modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login automatically disconnects. When prompted, enter **admin:**for the user name and **password** for the password. You can use procedures in the following sections to change the password and the amount of time for the administrator's login time-out.

Note: The user name and password are not the same as a user name or password you 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 and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

Changing the Built-In Password

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the modem router.
2. From the main menu, under the Maintenance heading, select **Set Password** to display the Set Password screen:
3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

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

Restricting Access by MAC Address

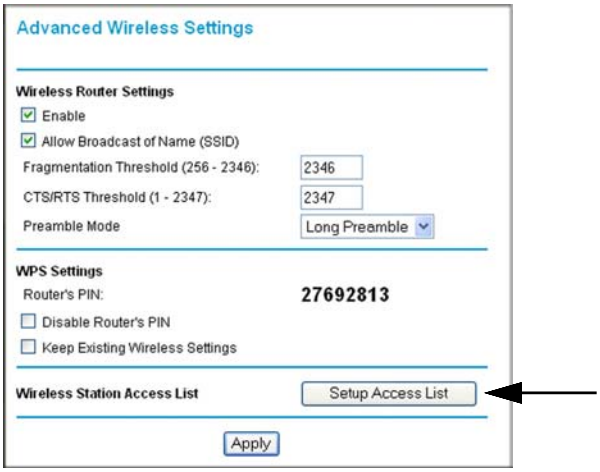
By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses.

To restrict access based on MAC addresses:

1. Log in to the modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin**, and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the modem router.

> **Note:** If you configure the router from a wireless computer, add your computer's MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the modem router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.

2. From the main menu, under the Advanced heading, select Wireless Settings, and then click **Setup Access List** to display the Wireless Card Access List screen.



Advanced Wireless Settings

Wireless Router Settings

☑ Enable

☑ Allow Broadcast of Name (SSID)

Fragmentation Threshold (256 - 2346): 2346

CTS/RTS Threshold (1 - 2347): 2347

Preamble Mode: Long Preamble

WPS Settings

Router's PIN: 27692813

□ Disable Router's PIN

□ Keep Existing Wireless Settings

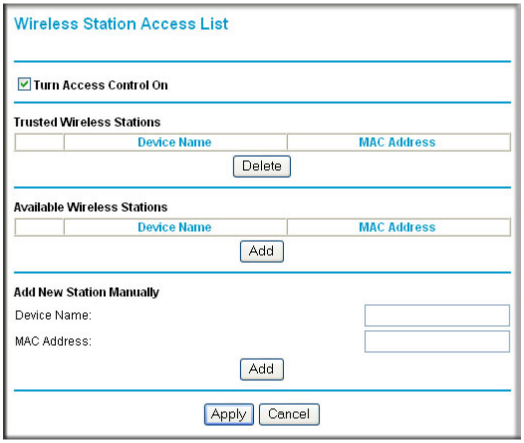
Wireless Station Access List: Setup Access List

Apply

Figure 3-1

The Wireless Station Access List screen displays a list of wireless PC's that are allowed to connect to the modem router based on their MAC addresses. These wireless PCs must also have the correct SSID and wireless security settings to access the wireless network.

3. Select the **Turn Access Control On** checkbox.



Wireless Station Access List

☑ Turn Access Control On

Trusted Wireless Stations

	Device Name	MAC Address

Available Wireless Stations

	Device Name	MAC Address

Add New Station Manually

Device Name:

MAC Address:

Figure 3-2

Note: If the **Turn Access Control On** checkbox is selected and the **Trusted Wireless Stations** list is blank; then no wireless PCs will be able to connect to your wireless network.

4. You can select a wireless station from the Available Wireless Stations list, or you can enter its MAC address manually:
   - If the wireless station is shown in the Available Wireless Stations list, click its radio button to select it, and then click **Add**.
   - To manually specify the wireless station, in the Add New Station Manually section, enter the name of the wireless station and its MAC address.The MAC address is 12 hexadecimal digits and can usually be found on the bottom of the wireless device. Click **Add**.

   The Wireless Station appears in the **Trusted Wireless Stations** list.

Note: You can use the **Delete** button to remove access by a wireless station.

5. When you are finished, click **Apply** to save your changes. Now, only devices on the Trusted Devices list will be allowed to wirelessly connect to the modem router.

Blocking Access to Internet Sites

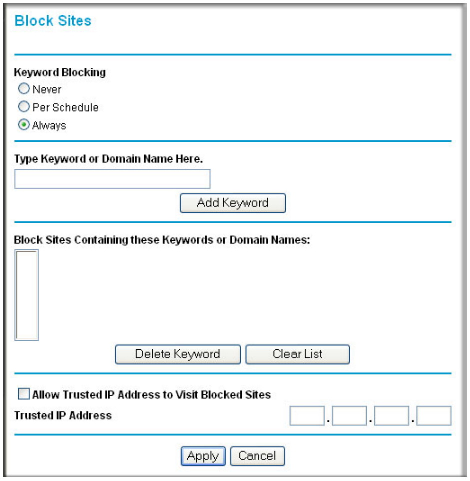
The modem router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list.

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 Security in the main menu. The Block Sites screen displays.



Block Sites

Keyword Blocking

○ Never
○ Per Schedule
● Always

Type Keyword or Domain Name Here.

Block Sites Containing these Keywords or Domain Names:

□ Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address

Figure 3-3

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 3-14.

   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 in 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.

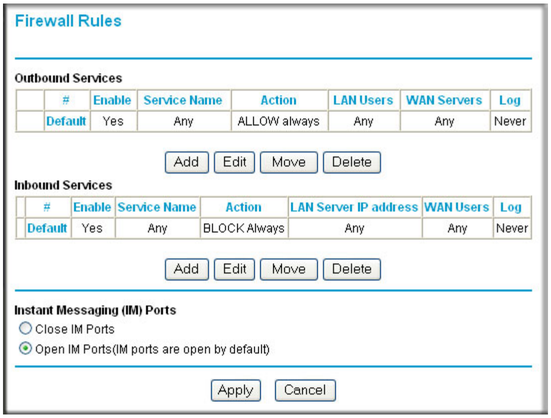
5. Click **Apply** to save all your settings in the Block Sites screen.

Firewall Rules

You can use this screen to create firewall rules to block or allow specific traffic. **This feature is for advanced administrators only!** Incorrect configuration will cause serious problems.

The Firewall Rules screen lists all existing rules for outbound traffic and inbound traffic. If you have not defined any rules, only the default rules are listed. You can add or edit rules. You can also use the **Move** and **Delete** buttons to move the selected rule to a new position in the table, or to delete the selected rule.

From the modem router menu, select Firewall Rules to display the following screen:.



Firewall Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
	Default	Yes	Any	ALLOW always	Any	Any	Never

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
	Default	Yes	Any	BLOCK Always	Any	Any	Never

Instant Messaging (IM) Ports

○ Close IM Ports

● Open IM Ports(IM ports are open by default)

Figure 3-4

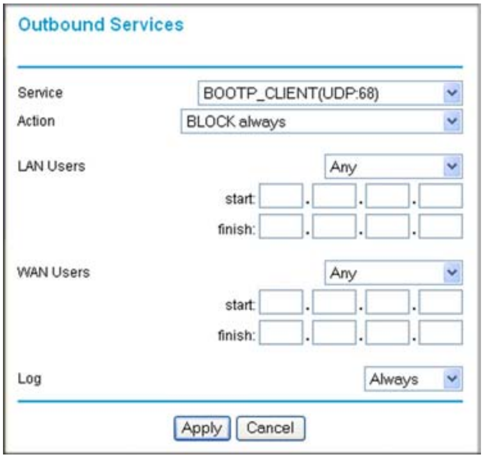
- **Outbound Services**. This lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic.
- **Inbound Services**. This lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

- Ports to enable MSN and AOL Instant Messaging are open by default. To close these ports, select the **Close IM Ports** radio button, and then click **Apply** so that your changes take effect. When these ports are closed Instant Messaging will not function.

To add or edit a rule from the Firewall Rules screen:

1. To edit a rule, select its radio button. To add a rule, click **Add** (it does not matter which radio button is selected).

   Depending on your selection, either the Outbound Services screen or Inbound Services screen is displayed.



Outbound Services

Service: BOOTP_CLIENT(UDP:68)
Action: BLOCK always
LAN Users: Any
start: . . .
finish: . . .
WAN Users: Any
start: . . .
finish: . . .
Log: Always

Figure 3-5

2. Select the service that you want to add or edit.
3. Enter the settings to specify the service (see Table 3-1 on page 3-8).
4. Click **Apply** to have your changes take effect.

   The new rule will be listed in the table when you return to the Firewall Rules screen.

Table 3-1. Adding or Editing Firewall Service Rules

Field	Outbound Rules	Inbound Rules
Action	• For Outbound rules, ALLOW rules are only useful if the traffic is already covered by a BLOCK rule. (That is, you want to allow a subset of traffic that is currently blocked by another rule.) • To define the schedule used in these selections, use the Schedule screen (see "Scheduling Blocking" on page 3-14).	• For Inbound rules, BLOCK rules are only useful if the traffic is already covered by an ALLOW rule. (That is, you want to block a subset of traffic that is currently allowed by another rule.) • To define the schedule used in these selections, use the Schedule screen (see "Scheduling Blocking" on page 3-14).
LAN users (Outbound Services only)	These settings determine which computers on your network are affected by this rule, based on their source (LAN) IP address. Select the desired option: • **Any**. All local IP addresses are covered by this rule. • **Address range**. If this option is selected, you must enter the **Start** and **Finish** fields. • **Single address**. Enter the required address in the **Start** fields.	
Send to LAN Server (Inbound Services only)		Enter the IP address of the PC or Server on your LAN that will receive the inbound traffic covered by this rule.
WAN Servers	These settings determine which Internet locations are covered by the rule, based on their destination (WAN) IP address. Select the desired option: • **Any**. All local IP addresses are covered by this rule. • **Address range**. If this option is selected, you must enter the **Start** and **Finish** fields. • **Single address**. Enter the required address in the **Start** fields.	
Log	This determines whether packets covered by this rule are logged. Select the desired action: • **Always**. Always log traffic considered by this rule, whether it matches or not. This is useful when debugging your rules. • **Never**. Never log traffic considered by this rule, whether it matches or not. • **Match**. Log traffic only it matches this rule. (The action is determined by this rule.) • **Not Match**. Log traffic that is considered by this rule, but does not match (The action is NOT determined by this rule.)	

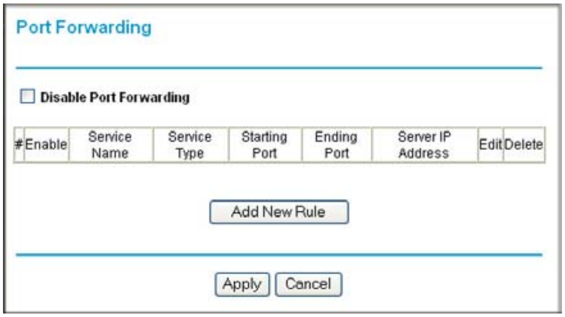
Port Forwarding

Using the port forwarding feature, 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 modem 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 "Configuring the WAN Setup Options" on page 6-7."

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.

Select Port Forwarding under Security in the main menu. The Port Forwarding screen displays:



Port Forwarding

□ Disable Port Forwarding

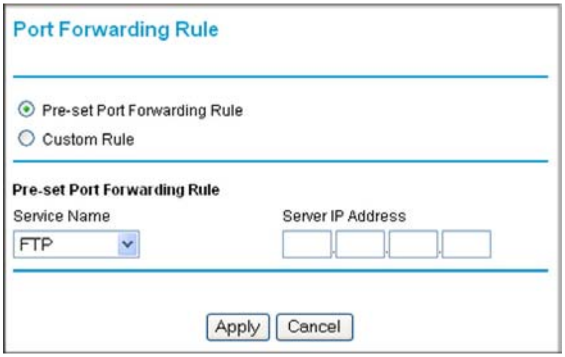
#	Enable	Service Name	Service Type	Starting Port	Ending Port	Server IP Address	Edit	Delete

Figure 3-6

You can add Pre-set Port Forwarding Rule or a Custom Rule.

Adding a Pre-set Port Forwarding Rule

1. From the Port Forwarding screen, click **Add** to display the following screen:



Port Forwarding Rule

● Pre-set Port Forwarding Rule

○ Custom Rule

Pre-set Port Forwarding Rule

Service Name: FTP

Server IP Address: □.□.□.□

Figure 3-7

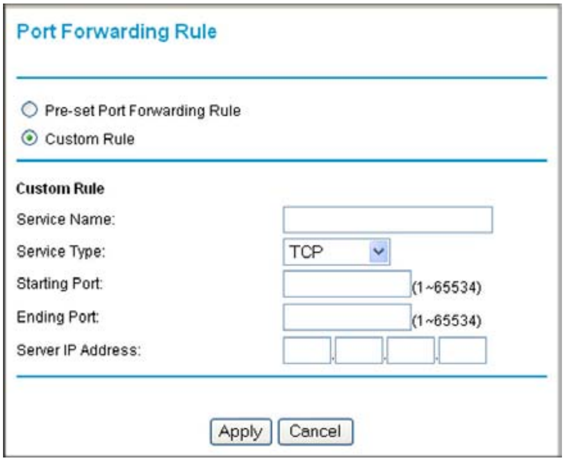
2. Select the rule from the drop-down **Service Name** list.

3. Fill in the Server IP Address field and then click **Apply**.

Adding a Custom Port Forwarding Rule

1. From the Port Forwarding screen, click **Add.**

2. Select the **Custom Rule** radio button and the screen changes:



Port Forwarding Rule

○ Pre-set Port Forwarding Rule

● Custom Rule

Custom Rule

Service Name: □

Service Type: TCP

Starting Port: □ (1~65534)

Ending Port: □ (1~65534)

Server IP Address: □.□.□.□

Figure 3-8

3. Enter a name in the **Service Name** field.

4. In the **Service Type** field, select the protocol. If you are unsure, select **TCP/UDP**.

5. Fill in the **Starting Port** and **Ending Port** fields.

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.

Port Triggering

Port triggering is an advanced feature that can be used to easily enable gaming and other Internet applications that would otherwise be blocked by the firewall. Using this feature requires that you know the port numbers that are used by the application.

Note: For information about port forwarding and port blocking, see "Firewall Rules" on page 3-6."

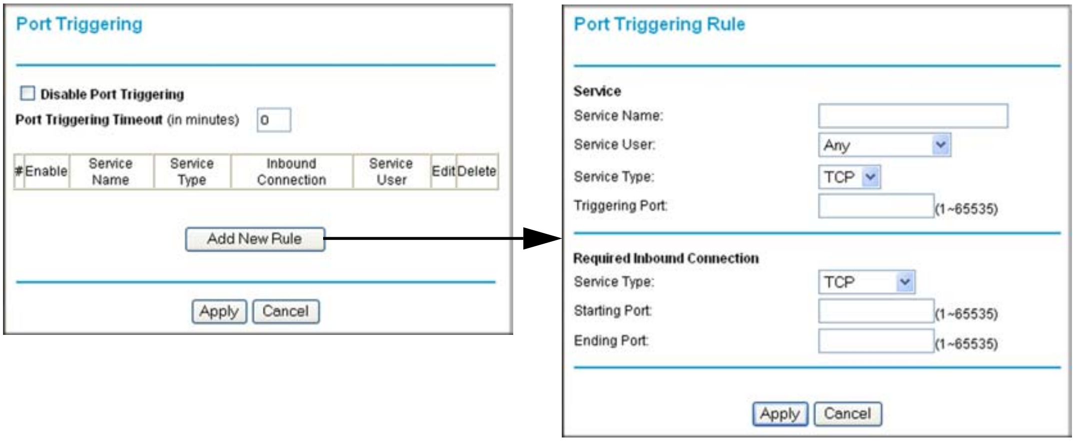
Once configured, port triggering operation is as follows:

1. A PC makes an outgoing connection using a port number defined in the Port Triggering table.
2. The modem router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering List, and associates them with the PC.
3. The remote system receives the PCs request, and responds using a different port number.
4. The modem router matches the response to the previous request, and forwards the response to the PC. (Without port triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the port forwarding rules.)

Note: Only one PC can use a port triggering application at any time. After a PC has finished using a port triggering application, there is a short time-out period before the application can be used by another PC.

To configure port triggering:

1. In the main menu, under Security, select Port Triggering. The Port Triggering screen displays.



Port Triggering

☐ Disable Port Triggering

Port Triggering Timeout (in minutes) 0

#	Enable	Service Name	Service Type	Inbound Connection	Service User	Edit	Delete

Add New Rule

Apply Cancel

Port Triggering Rule

Service

Service Name:

Service User: Any

Service Type: TCP

Triggering Port: (1~65535)

Required Inbound Connection

Service Type: TCP

Starting Port: (1~65535)

Ending Port: (1~65535)

Apply Cancel

Figure 3-9

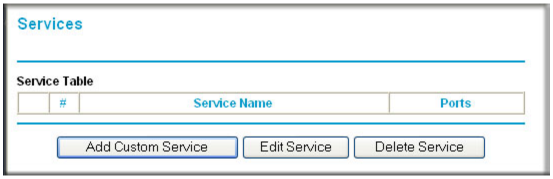
2. Specify the information for port triggering:
   - **Service Name**. Enter a name for the rule, up to 30 characters.
   - **Service User**. The PC on the LAN that can use the Port Triggering rule to create a dynamic inbound mapping to it. There are 2 options: (1) the Port Triggering rule is applied to all PCs on the LAN. That is, any PC on the LAN can use the rule and make the router to open a dynamic mapping to it. (2) The Port Triggering rule is only applied to the user specified PC on the LAN.
   - **Service Type**. Defines whether the traffic is TCP or UDP.
   - **Triggering Port**. The destination port number of the traffic. That is, when there is a packet from a LAN PC, which the rule is applied to, with the specified Service Type and destined to the specified Triggering Port, the router creates a dynamic mapping rule to the LAN PC.
   - **Required Inbound Connection**. This defines what the dynamic mapping is. The Connection Type defines whether the dynamic mapping is for TCP traffic, UDP traffic, or TCP and UDP traffic. The open port range is specified by the Starting Port and the Ending Port, and this defines the port(s) that the dynamic mapping is applied to.
3. Click **Apply** to save your settings and activate the port triggers that you have enabled.

Blocking Access to Internet Services

The modem router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

To block access to Internet services:

1. Select Services under Security in the main menu. The Services screen displays.



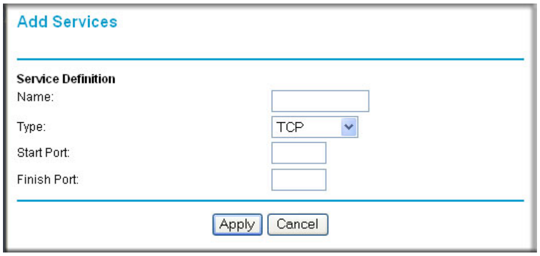
Services

Service Table

	#	Service Name	Ports

Figure 3-10

2. To add a service, click **Add Custom Service**. The following screen displays.



Add Services

Service Definition

Name:

Type: TCP

Start Port:

Finish Port:

Figure 3-11

3. Enter a name for the service.
4. From the **Service Type** drop-down list, select the application or service to be allowed or blocked. If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.
5. You can block the specified service for a single computer, a range of computers with consecutive IP addresses, or all computers on your network. Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both fields.

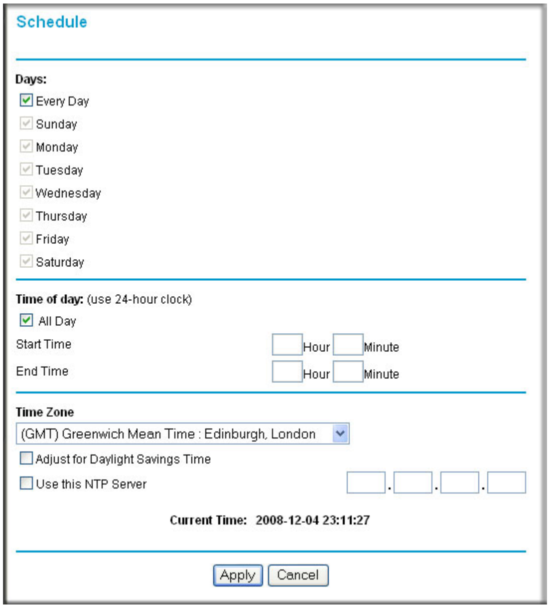
You must determine which port number or range of numbers is used by the application. The service port numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, “Assigned Numbers.” Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

6. Click **Apply** so that your changes take effect.

Scheduling Blocking

To schedule blocking:

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



Schedule

Days:

☑ Every Day

☑ Sunday

☑ Monday

☑ Tuesday

☑ Wednesday

☑ Thursday

☑ Friday

☑ Saturday

Time of day: (use 24-hour clock)

☑ All Day

Start Time □ Hour □ Minute

End Time □ Hour □ Minute

Time Zone

(GMT) Greenwich Mean Time : Edinburgh, London

□ Adjust for Daylight Savings Time

□ Use this NTP Server □.□.□.□

Current Time: 2008-12-04 23:11:27

Figure 3-12

2. Configure the schedule for blocking keywords and services.

a. Days. 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**. Select a start and end time in 24-hour format. Select **All Day** for 24-hour blocking. Click **Apply**.

Be sure to select your time zone in the E-mail screen as described in "Setting the Time" on page 3-18.

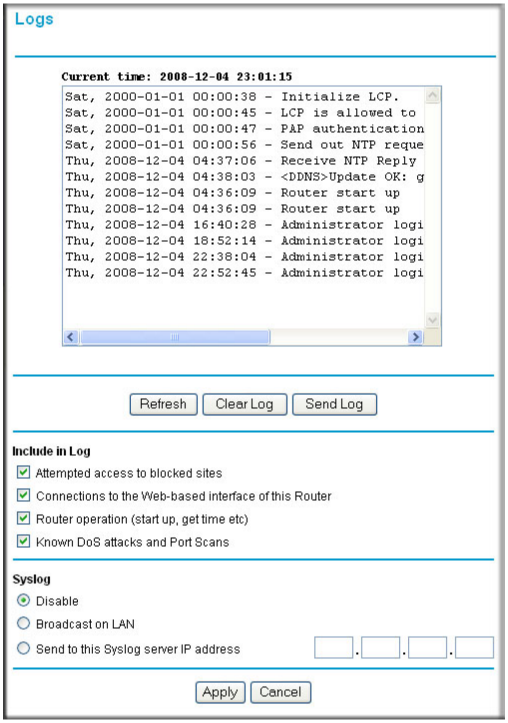
3. Click **Apply** to save your settings.

➡	**Note:** For information about setting the time, see "Setting the Time" on page 3-18.

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 Security in the main menu. The Logs screen displays.



Logs

Current time: 2008-12-04 23:01:15

```
Sat, 2000-01-01 00:00:38 - Initialize LCP.
Sat, 2000-01-01 00:00:45 - LCP is allowed to
Sat, 2000-01-01 00:00:47 - PAP authentication
Sat, 2000-01-01 00:00:56 - Send out NTP reque
Thu, 2008-12-04 04:37:06 - Receive NTP Reply
Thu, 2008-12-04 04:38:03 - <DDNS>Update OK: g
Thu, 2008-12-04 04:36:09 - Router start up
Thu, 2008-12-04 04:36:09 - Router start up
Thu, 2008-12-04 16:40:28 - Administrator logi
Thu, 2008-12-04 18:52:14 - Administrator logi
Thu, 2008-12-04 22:38:04 - Administrator logi
Thu, 2008-12-04 22:52:45 - Administrator logi
```

Include in Log

☑ Attempted access to blocked sites
☑ Connections to the Web-based interface of this Router
☑ Router operation (start up, get time etc)
☑ Known DoS attacks and Port Scans

Syslog

● Disable
○ Broadcast on LAN
○ Send to this Syslog server IP address ___ . ___ . ___ . ___

Figure 3-13

Table 3-2. Log Entry Descriptions

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.

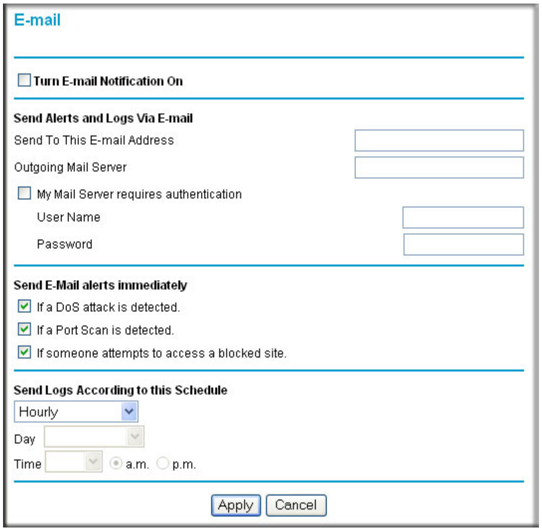
To e-mail the log immediately, click the **Send Log** button.

Configuring E-mail Alert and Web Access Log Notifications

To receive logs and alerts by e-mail, you must provide your e-mail account information.

To configure e-mail alert and web access log notifications:

1. Select **E-mail** under Security in the main menu. The E-mail screen displays.



E-mail

□ Turn E-mail Notification On

Send Alerts and Logs Via E-mail

Send To This E-mail Address

Outgoing Mail Server

□ My Mail Server requires authentication

User Name

Password

Send E-Mail alerts immediately

☑ If a DoS attack is detected.

☑ If a Port Scan is detected.

☑ If someone attempts to access a blocked site.

Send Logs According to this Schedule

Hourly

Day

Time ● a.m. ○ p.m.

Figure 3-14

2. To receive e-mail logs and alerts from the modem router, 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 e-mail program. If you leave this field blank, log and alert messages will not be sent by e-mail.

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

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

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

   b. Enter your password for the outgoing 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 router's memory. If the router cannot e-mail the log file, the log buffer might fill up. In this case, the modem 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 as described in the next section.

Setting the Time

The modem router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. To localize the time for your log entries, you must specify your time zone:

- **Time Zone**. Select your local time zone. This setting is used for the blocking schedule and for time-stamping log entries.
- **Adjust for Daylight Savings Time**. Select this check box when daylight savings time is in effect to adjust the time for your modem router.

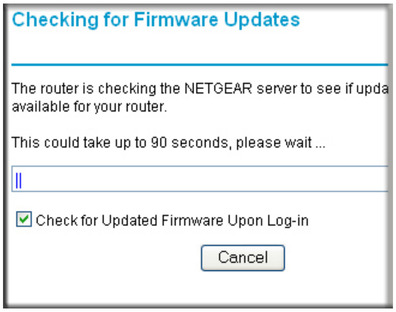
Chapter 4
Managing Your Network

This chapter describes features to help you manage your Dual Band Wireless-N Modem Router. This chapter includes the following sections:

- "Upgrading the Firmware"
- "Enabling Remote Management Access"
- "Viewing Modem Router Status Information" on page 4-4
- "Viewing a List of Attached Devices" on page 4-8
- "Managing the Configuration File" on page 4-9
- "Running Diagnostic Utilities and Rebooting the Modem Router" on page 4-10
- "Enabling Remote Management Access" on page 4-11

Upgrading the Firmware

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



Checking for Firmware Updates

The router is checking the NETGEAR server to see if upda
available for your router.

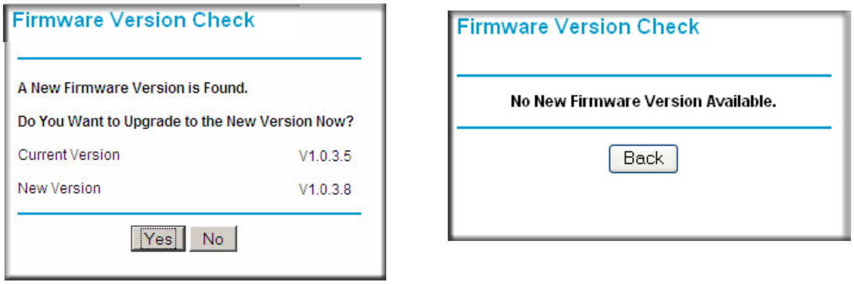
This could take up to 90 seconds, please wait ...

☑ Check for Updated Firmware Upon Log-in

Figure 4-1

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 modem 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.



Firmware Version Check

A New Firmware Version is Found.

Do You Want to Upgrade to the New Version Now?

Current Version	V1.0.3.5
New Version	V1.0.3.8

Firmware Version Check

No New Firmware Version Available.

Figure 4-2

To upgrade, click **Yes** to allow the modem router to download and install the new firmware.

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

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

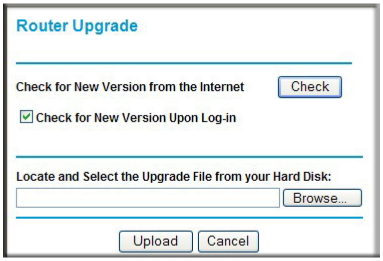
Manually Checking for Firmware Upgrades

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

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

1. Under Maintenance on the main menu, select Router Status. Note the version number of your modem router firmware.
2. Go to the DGND3300 support page on the NETGEAR website at *http://www.netgear.com/support*.

3. If the firmware version on the NETGEAR website is newer than the firmware on your modem router, download the file to your computer.
4. Under Maintenance on the modem router main menu, select Router Upgrade to display the following screen:



Router Upgrade

Check for New Version from the Internet [Check]

☑ Check for New Version Upon Log-in

Locate and Select the Upgrade File from your Hard Disk:

[Browse...]

[Upload] [Cancel]

Figure 4-3

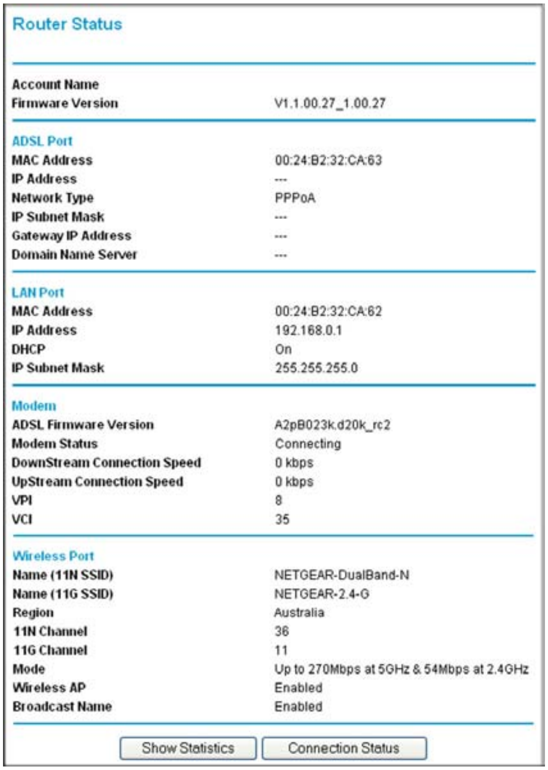
5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img or .chk).
6. Click **Upload** to send the firmware to the modem router.

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

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

Viewing Modem Router Status Information

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



Router Status

Account Name	
Firmware Version	V1.1.00.27_1.00.27
ADSL Port	
MAC Address	00:24:B2:32:CA:63
IP Address	---
Network Type	PPPoA
IP Subnet Mask	---
Gateway IP Address	---
Domain Name Server	---
LAN Port	
MAC Address	00:24:B2:32:CA:62
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
Modem	
ADSL Firmware Version	A2pB023k.d20k_rc2
Modem Status	Connecting
DownStream Connection Speed	0 kbps
UpStream Connection Speed	0 kbps
VPI	8
VCI	35
Wireless Port	
Name (11N SSID)	NETGEAR-DualBand-N
Name (11G SSID)	NETGEAR-2.4-G
Region	Australia
11N Channel	36
11G Channel	11
Mode	Up to 270Mbps at 5GHz & 54Mbps at 2.4GHz
Wireless AP	Enabled
Broadcast Name	Enabled

Figure 4-4

You can use the Show Statics and Connection Status buttons to view additional status information, as described in "Connection Status" on page 4-6 and "Statistics" on page 4-7. The following table explains Router Status screen fields.

Table 4-1. Modem Router Status Fields

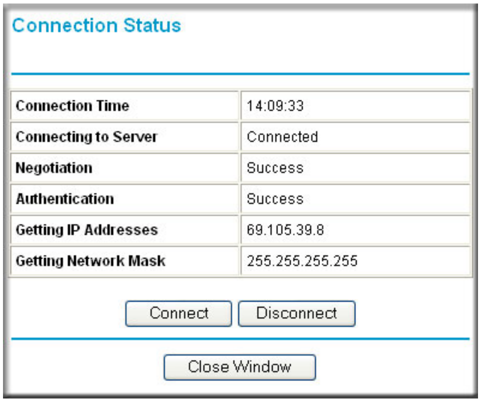
Field		Description
Account Name		The host name assigned to the modem router.
Firmware Version		The version of the modem router firmware. It changes if you upgrade the modem router.
Internet Port	MAC Address	The Media Access Control address. This is the unique physical address being used by the Internet (WAN) port of the modem router.
	IP Address	The IP address being used by the Internet (WAN) port of the modem router. If no address is shown, or is 0.0.0.0, the modem router cannot connect to the Internet.
	DHCP	• **None**. The modem router uses a fixed IP address on the WAN. • **DHCP Client**. The modem router obtains an IP address dynamically from the ISP.
	IP Subnet Mask	The IP subnet mask being used by the Internet (WAN) port of the modem router. For an explanation of subnet masks and subnet addressing, click the link to the online document "TCP/IP Networking Basics" in Appendix B.
	Domain Name Server	The Domain Name Server addresses being used by the modem router. A Domain Name Server translates human-language URLs such as www.netgear.com into IP addresses.
LAN Port	MAC Address	The Media Access Control address. This is the unique physical address being used by the Ethernet (LAN) port of the modem router.
	IP Address	The IP address being used by the Ethernet (LAN) port of the modem router. The default is 192.168.0.1.
	DHCP	Identifies whether the firmware's built-in DHCP server is active for the LAN-attached devices.
	IP Subnet Mask	The IP subnet mask being used by the Ethernet (LAN) port of the modem router. The default is 255.255.255.0.
Wireless Port	Name (11N SSID)	The 11N wireless network name (SSID) being used by the wireless port of the modem router. The default is NETGEAR-DualBand-N.
	Name (11G SSID)	The 11G wireless network name (SSID) being used by the wireless port of the modem router. The default is NETGEAR-2.4-G.
	Region	The geographic region where the modem router is being used. It might be illegal to use the wireless features of the modem router in some parts of the world.
	11N Channel	Identifies the 11N channel of the wireless port being used. Click the link to the online document "Wireless Networking Basics" in Appendix B for the frequencies used on each channel. In **Up to 270Mbps at 5GHz & 54Mbps at 2.4GHz** mode, there are two channels: a primary channel (P) and a secondary channel (S).

Table 4-1. Modem Router Status Fields (continued)

Field		Description
Wireless Port (continued)	11G Channel	Identifies the 11G channel of the wireless port being used. Click the link to the online document "Wireless Networking Basics" in Appendix B for the frequencies used on each channel. In **Up to 270Mbps at 2.4GHz** mode and **Up to 130Mbps at 2.4GHz** mode, the 11G channel is not active.
	Mode	Indicates the wireless communication mode: • Up to 270Mbps at 2.4GHz • Up to 270Mbps at 5GHz & 54Mbps at 2.4GHz (default) • Up to 130Mbps at 2.4GHz • Up to 130Mbps at 5GHz & 54Mbps at 2.4GHz
	Wireless AP	Indicates whether the radio feature of the modem router is enabled. If this feature is not enabled, the Wireless light on the front panel is off.
	Broadcast Name	Indicates whether the modem router is broadcasting its SSID.

Connection Status

To view the connection status, on the Router Status screen, click **Connection Status**.



Connection Status

Connection Time	14:09:33
Connecting to Server	Connected
Negotiation	Success
Authentication	Success
Getting IP Addresses	69.105.39.8
Getting Network Mask	255.255.255.255

Figure 4-5

- Click the **Connect** button, and the modem router attempts to connect to the Internet.
- Click the **Disconnect** button to disconnect the modem router Internet connection.
- Click the **Close Window** button to close the Connection Status screen.

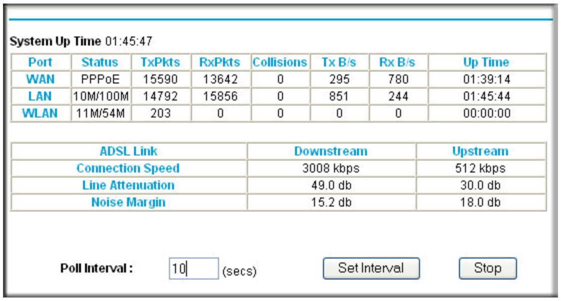
The following table describes the connection status settings.

Table 4-2. Connection Status Settings

Item	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.
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.

Statistics

To view statistics, on the Router Status screen, click **Show Statistics**.



System Up Time 01:45:47

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoE	15590	13642	0	295	780	01:39:14
LAN	10M/100M	14792	15856	0	851	244	01:45:44
WLAN	11M/54M	203	0	0	0	0	00:00:00

ADSL Link	Downstream	Upstream
Connection Speed	3008 kbps	512 kbps
Line Attenuation	49.0 db	30.0 db
Noise Margin	15.2 db	18.0 db

Poll Interval : 10 (secs)

Figure 4-6

The following table describes the modem router statistics.

Table 4-3. Modem Router Statistics

Item	Description
System Up Time	The time elapsed since the modem router was last restarted.
Port	The statistics for the WAN (Internet) and LAN (Ethernet) ports. For each port, the screen displays:

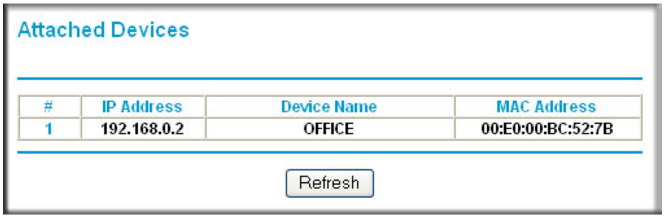
Table 4-3. Modem Router Statistics (continued)

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

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

Viewing a List of Attached Devices

The Attached Devices table lists all IP devices that the modem router has discovered on the local network. From the main menu, under Maintenance, select **Attached Devices** to view the table.



Attached Devices

#	IP Address	Device Name	MAC Address
1	192.168.0.2	OFFICE	00:E0:00:BC:52:7B

Figure 4-7

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 modem router to look for attached devices, click **Refresh**.

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

Managing the Configuration File

The configuration settings of the Dual Band Wireless-N Modem Router are stored within the modem router in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings. From the main menu, under Maintenance, select Backup Settings.

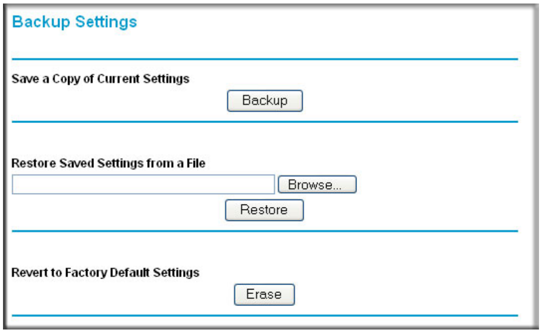

Backup Settings
Save a Copy of Current Settings
Backup
Restore Saved Settings from a File
Browse...
Restore
Revert to Factory Default Settings
Erase

Figure 4-8

The following sections describe the available options.

Backing Up and Restoring the Configuration

The Restore and Backup options in the Backup Settings screen let you save and retrieve a file containing your router's configuration settings.

To save your settings, click **Back Up**. Your browser extracts the configuration file from the router and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as comcast.cfg.

Tip: Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

To restore your settings from a saved configuration file, enter the full path to the file on your computer, or click **Browse** to browse to the file. When you have located it, click **Restore** to send the file to the modem router. The modem router then reboots automatically.

Warning: Do not interrupt the reboot process.

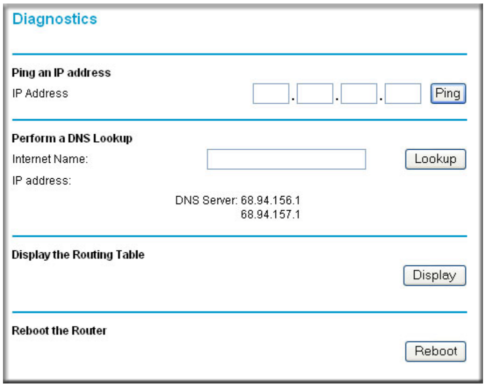
Erasing the Configuration

Under some circumstances (for example, if you move the modem router to a different network or if you have forgotten the password), you might want to erase the configuration and restore the factory default settings. After an erase, the modem router's user name is **admin**, the password is **password**, the LAN IP address is **192.168.0.1**, and its DHCP server is enabled.

- To erase the configuration, click the **Erase** button in the Backup Settings screen.
- To restore the factory default configuration settings when you do not know the login password or IP address, you must use the restore factory settings button on the rear panel of the modem router (see "Restoring the Factory Configuration Settings" on page A-1).

Running Diagnostic Utilities and Rebooting the Modem Router

The modem router has a diagnostics feature. In the main menu, under Maintenance, select Diagnostics to display the following screen.



Diagnostics

Ping an IP address

IP Address

Perform a DNS Lookup

Internet Name:

IP address:

DNS Server: 68.94.156.1
68.94.157.1

Display the Routing Table

Reboot the Router

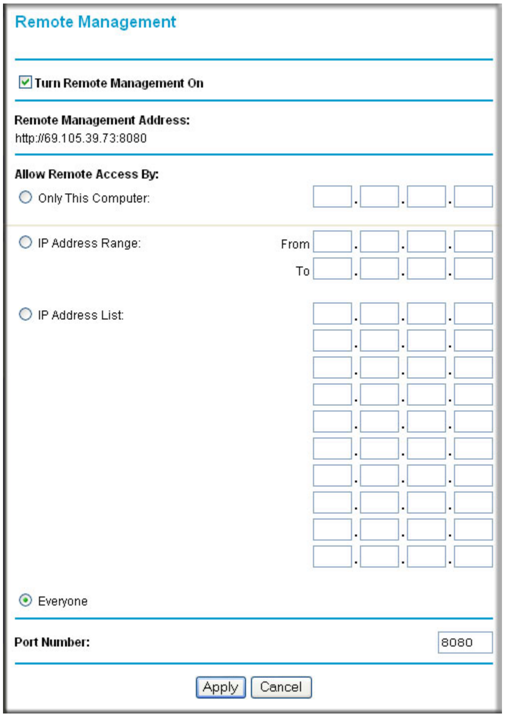
Figure 4-9

You can use the Diagnostics screen to perform the following functions from the modem router:

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

Enabling Remote Management Access

The remote management feature allows you to upgrade or check the status of your Dual Band Wireless-N Modem Router via the Internet. From the main menu, under Advanced, select Remote Management.



Remote Management

☑ Turn Remote Management On

Remote Management Address:
http://69.105.39.73:8080

Allow Remote Access By:

○ Only This Computer:

○ IP Address Range: From / To

○ IP Address List:

● Everyone

Port Number: 8080

Figure 4-10

Note: Be sure to change the modem 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 modem 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 modem router's remote management.

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

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

   Normal Web browser access 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 modem router from the Internet, type your modem router's WAN IP address into your browser's address or location field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, then enter **http://134.177.0.123:8080** in your browser.

Chapter 5
USB Storage

This chapter describes how to access and configure a USB storage drive attached to your modem router.

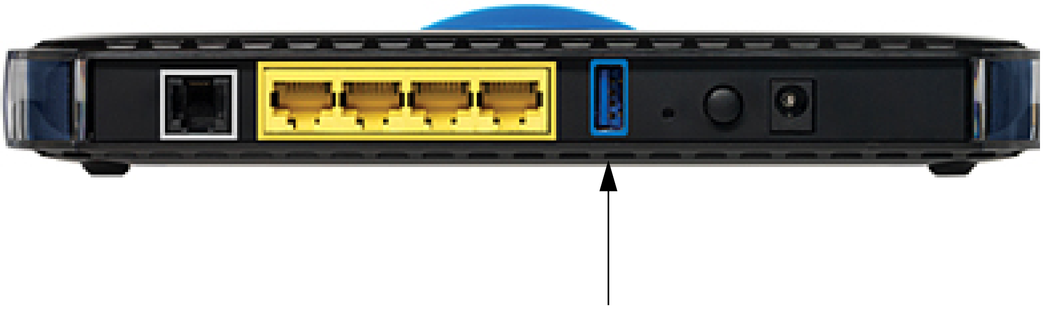


Figure 5-1

➡	**Note:** The USB port on the modem router can be used only to connect USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, printers, CD drives, or DVD drives to the modem router USB port.

This chapter includes the following sections:

- "USB Drive Requirements" on page 5-2
- "File Sharing Scenarios" on page 5-2
- "USB Storage Basic Settings" on page 5-4
- "Configuring USB Storage Advanced Settings" on page 5-8
- "Unmounting a USB Drive" on page 5-10
- "Specifying Approved USB Devices" on page 5-11
- "Connecting to the USB Drive from a Remote Computer" on page 5-12
- "Connecting to the USB Drive with Microsoft Network Settings" on page 5-12

USB Drive Requirements

The modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown below.

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

Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables.

The modem router should work with USB 2.0 or 1.1-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the modem router, go to: *http://kbserver.netgear.com/kb_web_files/n101300.asp*

When selecting a USB device, bear in mind the following:

- The USB port on the modem router can be used with one USB hard drive at a time. Do not attempt to use a USB hub attached to the USB port.
- Per the USB 2.0 specification, the maximum available power is 5V @ 0.5A. Some USB devices may exceed this requirement, in which case the device may not function or may function erratically. Check the documentation for your USB device to be sure.
- The modem router supports FAT, FAT32, NTFS (read only) and Linux file systems.

File Sharing Scenarios

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

- Sharing multimedia with friends and family — sharing MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network — storing files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and PC computers by using the USB drive as a go-between the systems.
- Sharing files with offsite coworkers — sharing files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Sharing Photos with Friends and Family

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

To share files with your friends and family:

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

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

2. If you want to specify read only access, or to allow access from the Internet, see "Configuring USB Storage Advanced Settings" on page 5-8.

Storing Files in a Central Location for Printing

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

- The daughter has some photos on her Macintosh computer that she wants to print.
- The mother has a photo-capable color printer directly attached to her PC, but not shared on the network.
- The mother and daughter's computers are not visible to each other on the network.

How can the daughter print her photos on the color printer attached to her mother's PC? This is where the USB drive on the modem router can save you time and effort.

1. The daughter accesses the USB drive by typing \\readyshare in the address field of her Web browser. Then she copies the photos to the USB drive.
2. The mother uses a her Web browser or Microsoft Networking to transfer the files from the USB drive to the PC. Then she prints the files.

Sharing Large Files with Colleagues

Sending files that are larger than 5 MB can pose a problem for many e-mail systems. The modem router allows you to share very large files such as PowerPoint presentations or ZIP files with colleagues at another site. Rather than tying up their mail systems will large files, your colleagues can use FTP to easily download shared files from the modem router.

Sharing files with a remote colleague involves the following steps:

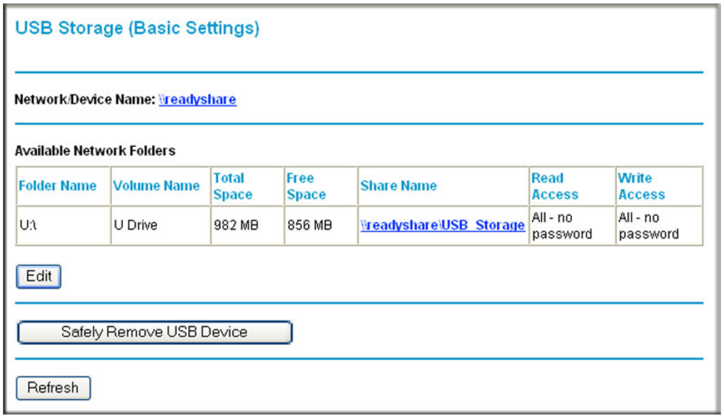
1. To protect your network, set up appropriate security. Create a user name and password for the colleague with appropriate access.
2. If you want to limit USB drive access to only Read Access, from the modem router USB Storage (Basic Settings) screen, click **Edit a Network folder**. In the Write Access field, select **admin**, and then click **Apply**.

> **Note:** The password for admin is the same one that you use to access the modem router. By default it is **password**.

3. Enable FTP via Internet in the USB Storage (Advanced Settings) screen. See "Configuring USB Storage Advanced Settings" on page 5-8.

USB Storage Basic Settings

You can view or edit basic settings for the USB storage device attached to your modem router. On the modem router main menu below the USB heading, select Basic Settings. The following screen displays:



USB Storage (Basic Settings)

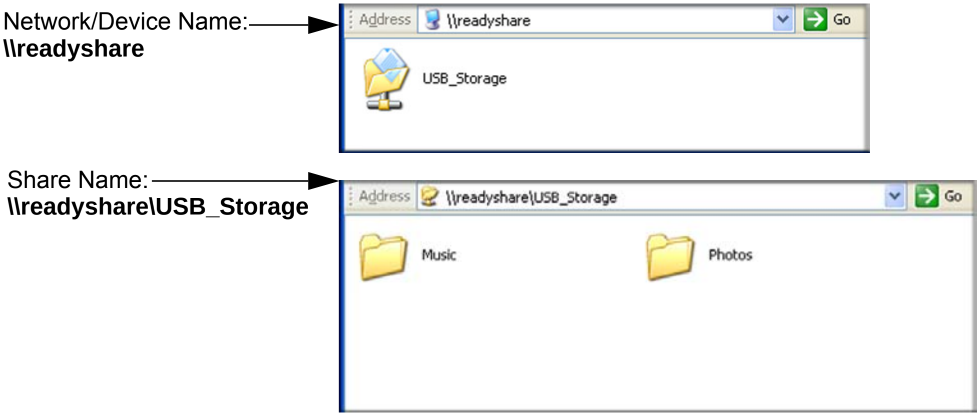
Network/Device Name: \\readyshare

Available Network Folders

Folder Name	Volume Name	Total Space	Free Space	Share Name	Read Access	Write Access
U:\	U Drive	982 MB	856 MB	\\readyshare\USB_Storage	All - no password	All - no password

Figure 5-2

By default, the USB storage device is available to all computers on your local area network (LAN). To access your USB device from this screen, you can click the **Network/Device Name** or the **Share Name**.


Network/Device Name:
\\readyshare

Share Name:
\\readyshare\USB_Storage

Figure 5-3

You can also type \\readyshare in the address field of your Web browser.

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

The following table explains the fields and buttons in this screen.

Table 5-1. USB Storage Basic Settings

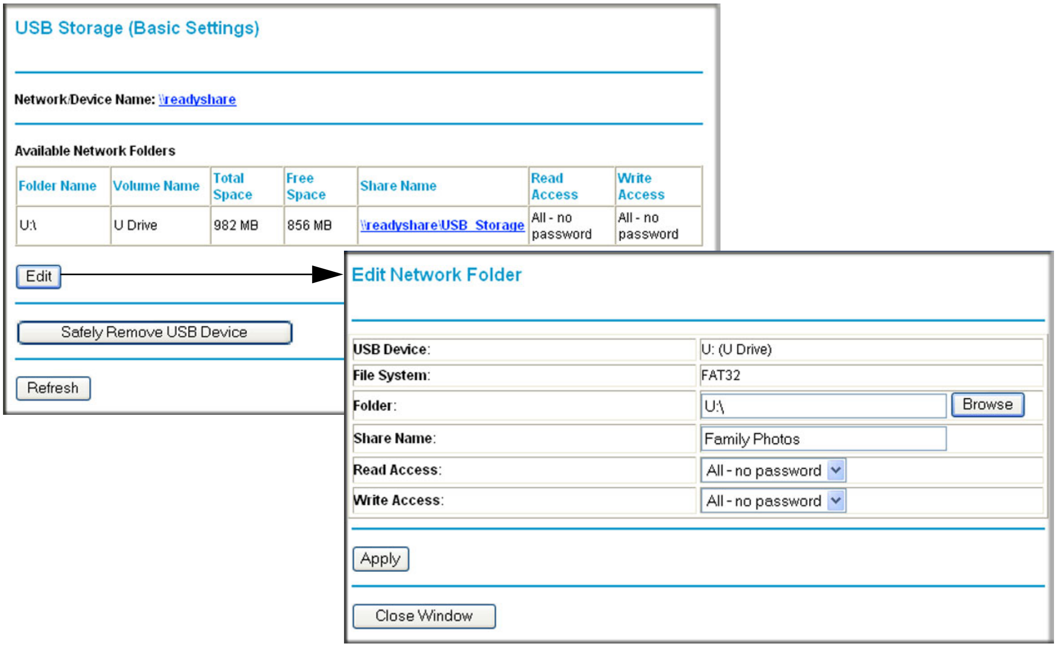
Fields and Buttons	Description
Network Device Name	The default is \\readyshare. This is the name used to access the USB device connected to the modem router.

Table 5-1. USB Storage Basic Settings

Fields and Buttons		Description
Available Network folders	Folder Name	Full path of the used by the Network Folder.
	Volume name	Volume name from the storage device (either USB drive or HDD).
	Total/Free Space	Shows the current utilization of the storage device.
	Share Name	• You can click the name shown or you can type it in the address field of your Web browser. • If Not Shared is shown then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
	Read/Write Access	• Shows the permissions/access controls on the network folder: • All -no password allows all users to access the network folder. • admin uses the same password that you use to log in to the modem router main menu.
Edit button		You can click the **Edit** button to edit the Available Network folder settings. See "Editing a Network Folder" on page 5-7.
Safely Remove USB Device button		Click to safely remove the USB device attached to your modem router. See "Unmounting a USB Drive" on page 5-10.

Editing a Network Folder

This process is the same from either the USB Storage (Basic Settings) screen or the USB Storage (Advanced Settings) screen. Click the **Edit** button to open the Edit Network Folder screen:



USB Storage (Basic Settings)

Network/Device Name: \\readyshare

Available Network Folders

Folder Name	Volume Name	Total Space	Free Space	Share Name	Read Access	Write Access
U:\	U Drive	982 MB	856 MB	\\readyshare\USB_Storage	All - no password	All - no password

Edit Network Folder

USB Device:	U: (U Drive)
File System:	FAT32
Folder:	U:\
Share Name:	Family Photos
Read Access:	All - no password
Write Access:	All - no password

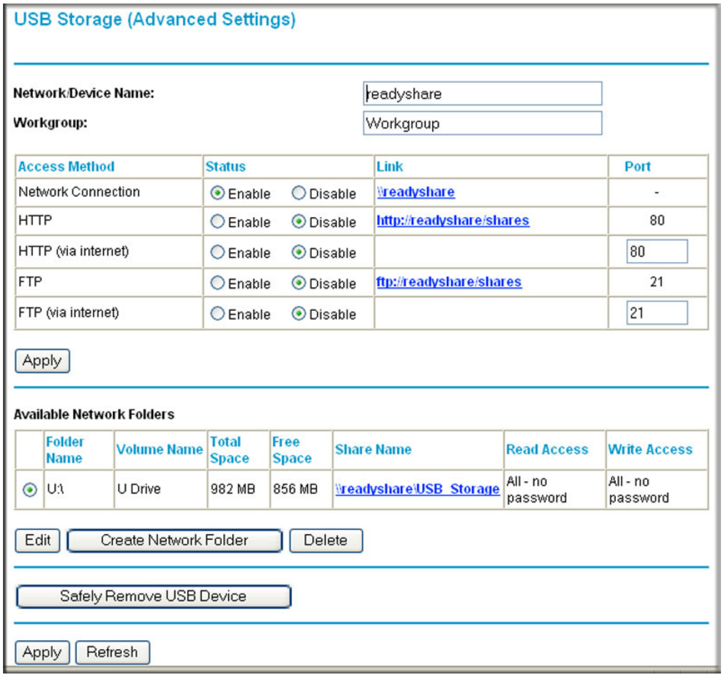
Figure 5-4

You can use this screen to select a folder, to change the **Share Name**, or to change the **Read Access** or **Write Access** from **All-no password** to **admin**. The password for **admin** is the same one that is used to log in to the modem router main menu. By default it is **password**.

Note: You must click **Apply** in order for your changes to take effect.

Configuring USB Storage Advanced Settings

To configure advanced USB settings, under the USB heading on the modem router main menu, select Advanced Settings. The USB Storage (Advanced Settings) screen displays:



USB Storage (Advanced Settings)

Network/Device Name: readyshare

Workgroup: Workgroup

Access Method	Status	Link	Port
Network Connection	● Enable ○ Disable	\\readyshare	-
HTTP	○ Enable ● Disable	http://readyshare/shares	80
HTTP (via internet)	○ Enable ● Disable		80
FTP	○ Enable ● Disable	ftp://readyshare/shares	21
FTP (via internet)	○ Enable ● Disable		21

Available Network Folders

	Folder Name	Volume Name	Total Space	Free Space	Share Name	Read Access	Write Access
●	U:\	U Drive	982 MB	856 MB	\\readyshare\USB_Storage	All - no password	All - no password

Figure 5-5

You can use this screen to specify access to the USB storage device. The following table explains the fields and buttons in the USB Storage Advanced Settings screen.

Table 5-2. USB Storage Advanced Settings

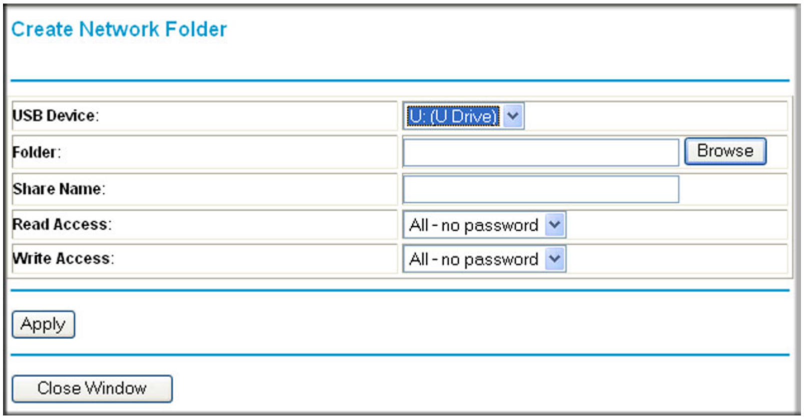
Fields	Description
Network Device Name	The default is readyshare. This is the name used to access the USB device connected to the modem router from your computer.
Workgroup	If you are using a Windows Workgroup rather than a domain, the Workgroup name is displayed here.

Table 5-2. USB Storage Advanced Settings (continued)

Fields		Description
Access Method	Network Connection	Enabled by default, this allows all users on the LAN to have access to the USB drive.
	HTTP	Disabled by default. If you enable this setting, you can type http://readyshare to access the USB drive.
	HTTP (via Internet)	Disabled by default. If you enable this settings, remote users can type http://readyshare to access the USB drive over the Internet.
	FTP	Disabled by default.
	FTP (via Internet)	Disabled by default. If you enable this settings, remote users can access the USB drive via ftp over the Internet.
Available Network Folders	Folder Name	Full path of the used by the Network Folder.
	Volume name	Volume name from the storage device (either USB drive or HDD).
	Total/Free Space	The current utilization of the storage device.
	Share Name	• You can click the name shown or you can type it into the address field of your Web browser. • If Not Shared is shown then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
	Read/Write Access	• Shows the permissions/access controls on the Network Folder: • All -no password allows all users to access the Network Folder. • admin prompts you to enter the same password that you use to log in to the modem router main menu.

Creating a Network Folder

From the USB Storage (Advanced Settings) screen. Click the **Create a Network Folder** button to open the Create a Network Folder screen:



Create Network Folder

USB Device:	U: (U Drive)
Folder:	Browse
Share Name:	
Read Access:	All - no password
Write Access:	All - no password

Figure 5-6

You can use this screen to create a folder and to specify its **Share Name**, **Read Access**, and **Write Access** from **All-no password** to **admin**. The password for **admin** is the same one that is used to log in to the modem router main menu. By default it is **password**.

➡ **Note:** You must click **Apply** in order for your changes to take effect.

Unmounting a USB Drive

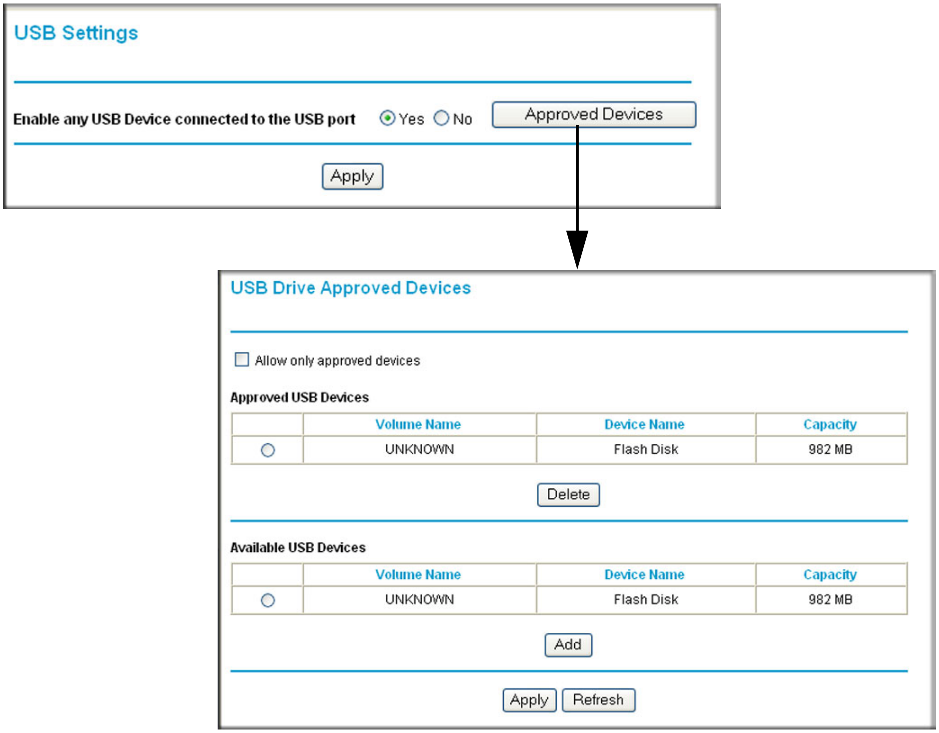
⚠ **Warning:** Unmount the USB drive first before physically unplugging it from the modem router. If the USB disk is removed or a cable is pulled while data is being written to the disk, it could result in file or disk corruption.

To unmount a USB disk drive so that no users can access it, from the USB Settings screen, click the **Safely Remove USB** button. This takes the drive offline.

Specifying Approved USB Devices

You can specify which USB devices are approved for use when connected to the modem router.

1. Under the Advanced Heading, select USB Settings from the main menu, and then click **Approved Devices**. The USB Drive Approved Settings screen displays:



USB Settings

Enable any USB Device connected to the USB port ● Yes ○ No

USB Drive Approved Devices

□ Allow only approved devices

Approved USB Devices

	Volume Name	Device Name	Capacity
○	UNKNOWN	Flash Disk	982 MB

Available USB Devices

	Volume Name	Device Name	Capacity
○	UNKNOWN	Flash Disk	982 MB

Figure 5-7

2. Select the USB device from the **Available USB Devices** list.
3. Click **Add**.
4. Select the **Allow only approved devices** check box.
5. Click **Apply** so that your change goes into effect.

If you want to approve another USB device, you must first use the **Safely Remove USB Device** button to unmount the currently connected USB device. Connect the other USB device, and then repeat this process.

Connecting to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers using a Web browser, you must use the router’s Internet port IP address.

Locating the Internet Port IP Address

The Router Status screen shows the Internet port IP address:

1. Log in to the modem router.
2. Under the Maintenance section in the left navigator, click **Router Status**.
3. Record the IP address that is listed for the Internet Port. This is the IP address you can use to connect to the router remotely.

Accessing the Router’s USB Drive Remotely Using FTP

You can connect to the router’s USB drive using a Web browser:

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

   ftp://10.1.65.4 If you are using dynamic DNS, you can type the DNS name rather than the IP address.
2. Type the account name and password that has access rights to the USB drive.
3. The directories of the USB drive that your account has access to will be displayed, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Connecting to the USB Drive with Microsoft Network Settings

You can access the USB drive from local computers on your home or office network using Microsoft network settings. You must be running Microsoft Windows 2000, XP, or older versions of Windows with Microsoft networking enabled. You can use normal Explorer operations such as drag and drop, file open, or cut/paste files from:

- Microsoft Windows Start Menu, Run option
- Windows Explorer

- Network Neighborhood or My Network Place

Enabling File and Printer Sharing

Each computer’s network properties must be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft Networks must be enabled, as described below.

> **Note:** In Windows 2000 and Windows XP, File and Printer Sharing is enabled by default.

Configuring Windows 98SE and Windows ME

The easiest way to get to your network properties is to go to your desktop, right-click Network Neighborhood and then click Properties. File and printer sharing for Microsoft Windows should be listed. If not, click Add and follow the installation prompts.

> **Note:** **Note:** If you have any questions on File and Printer Sharing, please contact Microsoft for assistance.

Configuring Windows 2000 and Windows XP

Right-click on the network connection for your local area network. File and Printer Sharing for Microsoft Windows should be listed. If not, click Install and follow the installation prompts.

Chapter 6
Customizing Your Network Settings

This chapter describes advanced features of the RangeMax Dual Band Wireless-N Modem Router. This chapter includes the following sections:

- “Using the LAN Setup Options
- “Configuring the WAN Setup Options” on page 6-7
- “Setting up Quality of Service (QoS)” on page 6-9
- “Using a Dynamic DNS Service” on page 6-5
- “Configuring Static Routes” on page 6-14
- “Wireless Repeating (Also Called WDS)” on page 6-16

Using the LAN Setup Options

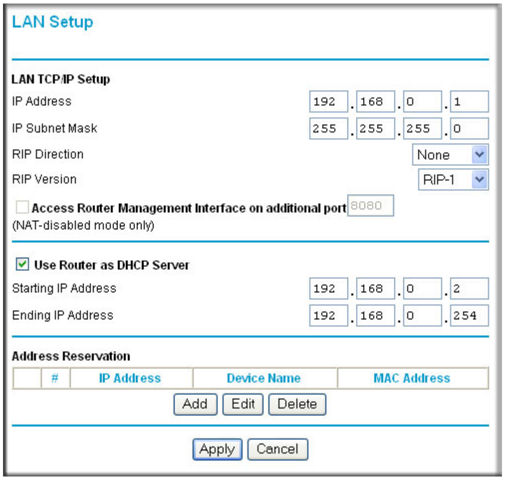
The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

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

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

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

To configure LAN settings, log in to the modem router, and under the Advanced heading, select LAN Setup. The following screen displays:



LAN Setup

LAN TCP/IP Setup

IP Address 192 . 168 . 0 . 1

IP Subnet Mask 255 . 255 . 255 . 0

RIP Direction None

RIP Version RIP-1

□ Access Router Management Interface on additional port 8080
(NAT-disabled mode only)

☑ Use Router as DHCP Server

Starting IP Address 192 . 168 . 0 . 2

Ending IP Address 192 . 168 . 0 . 254

Address Reservation

	#	IP Address	Device Name	MAC Address

Figure 6-1

If you make changes you must click **Apply** in order for the changes to take effect.

> **Note:** If you change the LAN IP address of the modem 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 LAN Setup fields are explained in the following table.

Table 6-1. LAN Setup

Settings	Description
Device Name	A descriptive name for the modem router, which will be shown in the Network on Windows Vista and the Network Explorer on all Windows systems. The **Device Name** field cannot be blank.

Table 6-1. LAN Setup

Settings		Description
LAN TCP/IP Setup	IP Address	The LAN IP address of the modem router.
	IP Subnet Mask	The LAN subnet mask of the modem router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router.
	RIP Direction	RIP (Router Information Protocol) allows a modem router to exchange routing information with other routers. This setting controls how the modem router sends and receives RIP packets. **Both** is the default. • **Both** or **Out Only**. The modem router broadcasts its routing table periodically. • **Both** or **In Only**. The modem router incorporates the RIP information that it receives. • **None**. The modem router will not send any RIP packets and will ignore any RIP packets received.
	RIP Version	This controls the format and the broadcasting method of the RIP packets that the modem router sends. It recognizes both formats when receiving. By default, this is **RIP-1**. • RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup. • RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.
DHCP Server For more information	Use Router as a DHCP Server	This check box is usually selected so that the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server. See "Using the Modem Router as a DHCP Server" on page 6-4.
	Starting IP Address	Specify the start of the range for the pool of IP addresses in the same subnet as the modem router.
	Ending IP Address	Specify the end of the range for the pool of IP addresses in the same subnet as the modem router.
Address Reservation For more information, see "Address Reservation" on page 6-4.		When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it access the modem router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

Using the Modem Router as a DHCP Server

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

For most applications, the default DHCP and TCP/IP settings of the modem 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.

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 modem router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you might wish to save part of the range for devices with fixed addresses.

The modem 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 modem router's LAN IP address)
- Primary DNS Server (if you entered a primary DNS address in the Basic Settings screen; otherwise, the modem 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 configure 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 will need to set your computers' IP addresses manually or they will not be able to access the modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the modem 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 **Add**.

2. In the **IP Address** field, type the IP address to assign to the computer or server. (Choose an IP address from the modem router’s LAN subnet, such as **192.168.0.x**.)
3. Type the MAC address of the computer or server.

> **Tip:** If the computer is already present on your network, 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 modem 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. Select the radio button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

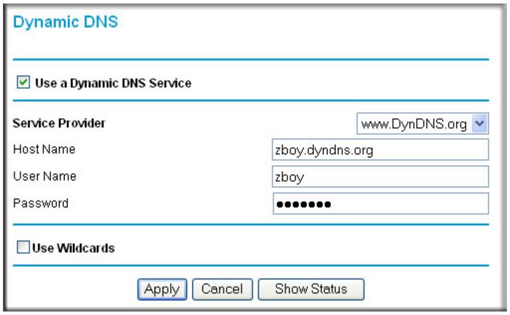
Using a Dynamic DNS Service

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 modem 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 configure in the modem router. Then, whenever your ISP-assigned IP address changes, your modem 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 modem router at hostname.dyndns.org.

From the main menu, under Advanced, select **Dynamic DNS** to display the Dynamic DNS screen.



Dynamic DNS

☑ Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name: zboy.dyndns.org

User Name: zboy

Password: ●●●●●●●●

□ Use Wildcards

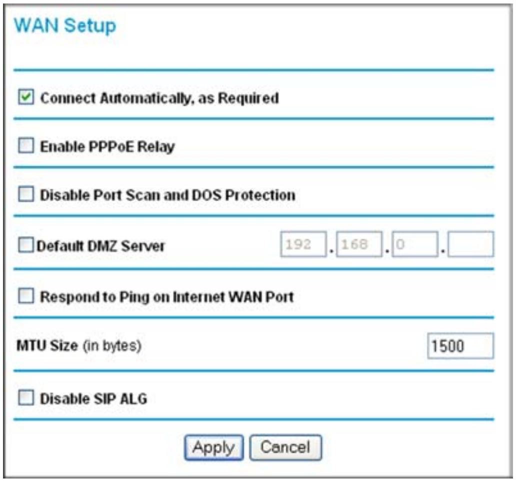
Figure 6-2

To configure Dynamic DNS:

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

Configuring the WAN Setup Options

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the Maximum Transmit Unit (MTU) size, and enable the modem router to respond to a ping on the WAN (Internet) port. From the main menu, under Advanced, click **WAN Setup** to view the WAN Setup screen.



WAN Setup

☑ Connect Automatically, as Required

□ Enable PPPoE Relay

□ Disable Port Scan and DOS Protection

□ Default DMZ Server 192 . 168 . 0 .

□ Respond to Ping on Internet WAN Port

MTU Size (in bytes) 1500

□ Disable SIP ALG

Figure 6-3

The WAN Setup fields are described in the following table:

Table 6-2. WAN Setup Settings

Setting	Description
Connect Automatically, as Required	Usually, this check box is selected, so that an Internet connection is made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can clear the check box to disable this feature. If this setting is disabled, you must connect manually, using the screen that you access by clicking the **Connection Status** button on the Status screen. If you have an Always on connection, this setting has no effect.
Enable PPPoE Relay	Selecting this check box allows a PPPoE client on a local PC to connect to a remote PPPoE server with the modem router acting as a relay agent.
Disable Port Scan and DOS Protection	The firewall protects your LAN against port scans and denial of service (DOS) attacks. This protection should be disabled only in special circumstances.

Table 6-2. WAN Setup Settings

Setting	Description
Default DMZ Server	This feature is sometimes helpful when you are using some online games and videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, Configuring Static Routes.
Respond to Ping on Internet WAN Port	If you want the modem router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, since it allows your modem router to be discovered. Do not select this check box unless you have a specific reason to do so.
MTU Size (in bytes)	The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 Bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection. See "Changing the MTU Size" on page 7-6.
Disable SIP ALG	The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The **Disable SIP ALG** check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

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

⚠ **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 modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding 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. In the last **Default DMZ Server** field, type the last digit of the IP address for that computer. To remove the default DMZ server, enter 0 (zero).
2. Select the **Default DMZ Server** check box, and click **Apply**.

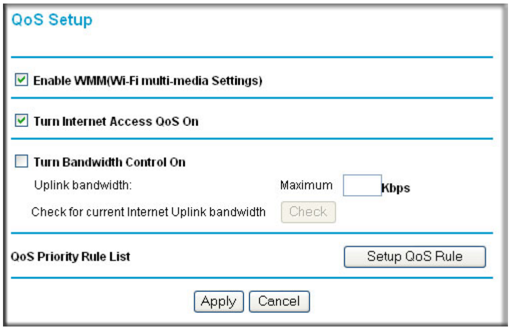
Setting up Quality of Service (QoS)

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

The modem router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both 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 add or create a policy for the type of traffic. To go to the QoS Setup screen, from the main menu, under Advanced, select **QoS Setup**.



QoS Setup

☑ Enable WMM(Wi-Fi multi-media Settings)

☑ Turn Internet Access QoS On

☐ Turn Bandwidth Control On

Uplink bandwidth: Maximum ☐ Kbps

Check for current Internet Uplink bandwidth

QoS Priority Rule List

Figure 6-4

WMM QoS is enabled by default. You can disable it by selecting QoS Setup from the main menu, clearing the **Enable WMM (Wi-Fi multi-media Settings)** check box and clicking **Apply**.

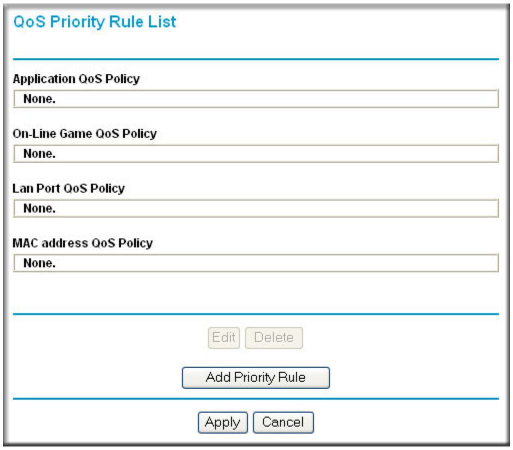
You can give prioritized Internet access to the following types of traffic:

- For specific applications or online games see "QoS for Applications and Online Gaming" on page 6-10.
- For QoS on individual Ethernet LAN ports of the modem router, see "QoS for a Router LAN Port" on page 6-12.
- For QoS from a specific device by MAC address, see "QoS for a MAC Address" on page 6-12.

QoS for Applications and Online Gaming

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

1. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays.
2. Click **Setup QoS rule**. The QoS - Priority Rules screen displays.



QoS Priority Rule List

Application QoS Policy: None.

On-Line Game QoS Policy: None.

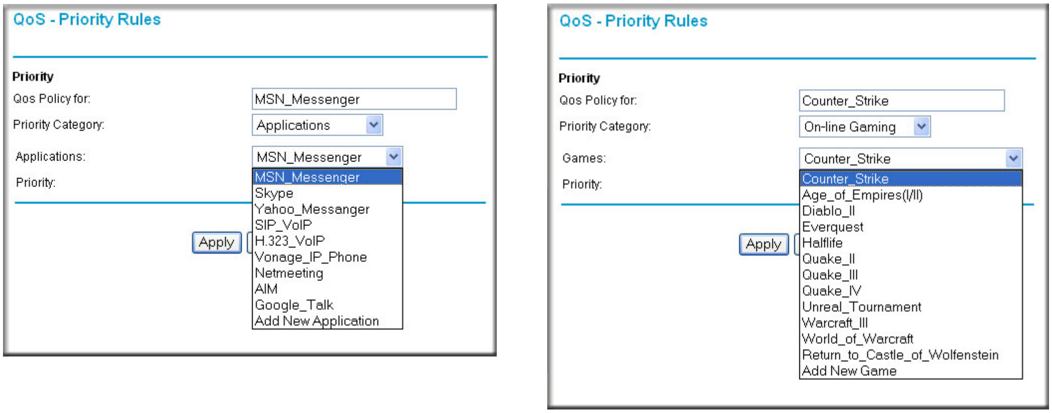
Lan Port QoS Policy: None.

MAC address QoS Policy: None.

Figure 6-5

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

4. In the **Priority Category** field, either use the default selection of **Applications,** or select **Online Gaming**. A drop-down list of predefined applications or games is available.



QoS - Priority Rules

Priority

Qos Policy for: MSN_Messenger

Priority Category: Applications

Applications: MSN_Messenger

Priority:

QoS - Priority Rules

Priority

Qos Policy for: Counter_Strike

Priority Category: On-line Gaming

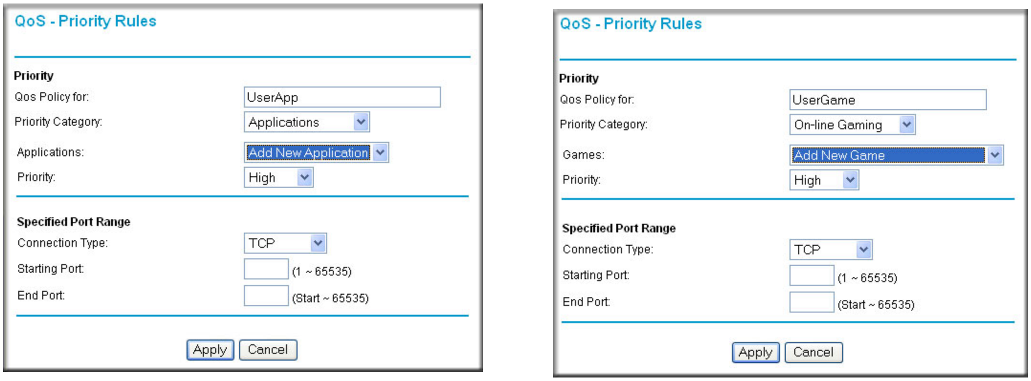
Games: Counter_Strike

Priority:

Figure 6-6

5. 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:



QoS - Priority Rules

Priority

Qos Policy for: UserApp

Priority Category: Applications

Applications: Add New Application

Priority: High

Specified Port Range

Connection Type: TCP

Starting Port: (1 ~ 65535)

End Port: (Start ~ 65535)

QoS - Priority Rules

Priority

Qos Policy for: UserGame

Priority Category: On-line Gaming

Games: Add New Game

Priority: High

Specified Port Range

Connection Type: TCP

Starting Port: (1 ~ 65535)

End Port: (Start ~ 65535)

Figure 6-7

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

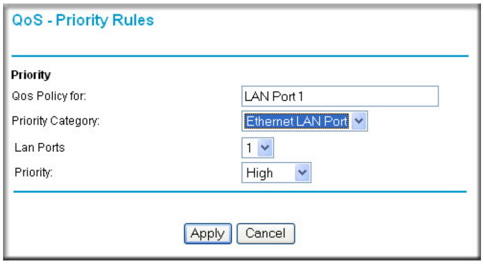
   c. Select the Connection Type, either **TCP, UDP,** or both (**TCP/UDP**), and specify the port number or range of port numbers used by the application or game.

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. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays.
2. Click **Setup QoS Rule**.
3. In the **Priority Category** field, select **Ethernet LAN Port**. The screen changes:



QoS - Priority Rules

Priority

Qos Policy for: LAN Port 1

Priority Category: Ethernet LAN Port

Lan Ports: 1

Priority: High

Figure 6-8

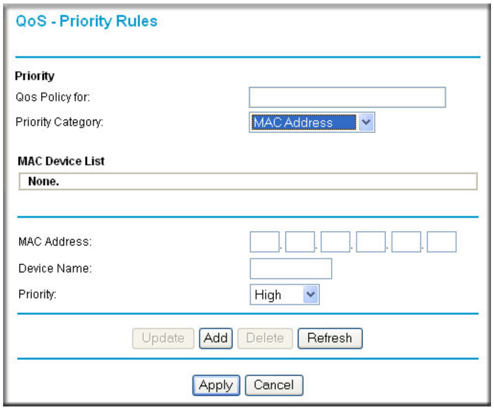
4. In the **LAN port** field, select the LAN port that will have a QoS policy.
5. From the **Priority** drop-down list, select the priority that this port's traffic should receive relative to other applications and traffic when accessing the Internet. The options are Low, Normal, High, and Highest.
6.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

QoS for a MAC Address

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

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

2. Click **Add Priority Rule**.
3. In the **Priority Category** field, select **MAC Address**. The screen changes:



QoS - Priority Rules

Priority

Qos Policy for:

Priority Category: MAC Address

MAC Device List

None.

MAC Address:

Device Name:

Priority: High

Figure 6-9

4. 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.
5. 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.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
8. Click **Apply**.

Editing or Deleting an Existing QoS Policy

To edit or delete an existing QoS policy:

1. From the main menu, under Advanced, select **QoS Setup**. The QoS Setup screen displays.
2. Select the radio button for the QoS policy to be edited or deleted, and do one of the following:
   - Click **Delete** to remove the QoS policy.
   - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.

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

Configuring Static Routes

Static routes provide additional routing information to your modem router. Under usual circumstances, the modem 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 192.168.0.100.
- Your company's network address is 134.177.0.0.

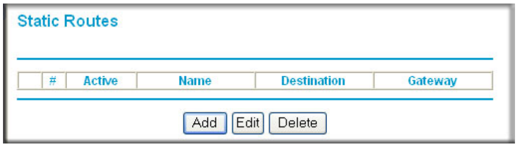
When you first configured your modem router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your modem 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 modem router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100.

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 192.168.0.100.
- 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.

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



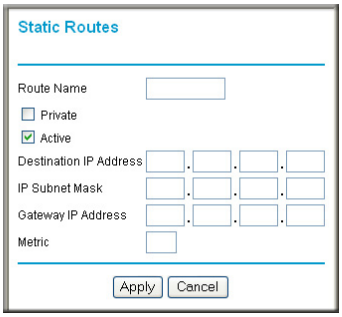
Static Routes

	#	Active	Name	Destination	Gateway

Figure 6-10

To add or edit a static route:

1. Click **Add** to open the Static Routes screen.



Static Routes

Route Name

□ Private

☑ Active

Destination IP Address . . .

IP Subnet Mask . . .

Gateway IP Address . . .

Metric

Figure 6-11

2. In the **Route Name** field, type a name for this static route. (This is for identification purposes only.)
3. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.
4. Select the **Active** check box to make this route effective.
5. Type the destination IP address of the final destination.
6. Type the IP subnet mask for this destination.
   If the destination is a single host, type 255.255.255.255.
7. Type the gateway IP address, which must be a router on the same LAN segment as the Dual Band Wireless-N Modem Router.
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.

Wireless Repeating (Also Called WDS)

The Dual Band Wireless-N Modem Router can be used with a wireless access point (AP) to build large bridged wireless networks. Wireless repeating is a type of Wireless Distribution System (WDS).

⚠	**Warning:** If you use the wireless repeating function, your options for wireless security are limited to None or WEP. For more information about wireless security, see Chapter 2, "Safeguarding Your Network."

The following figure shows a wireless repeating scenario:

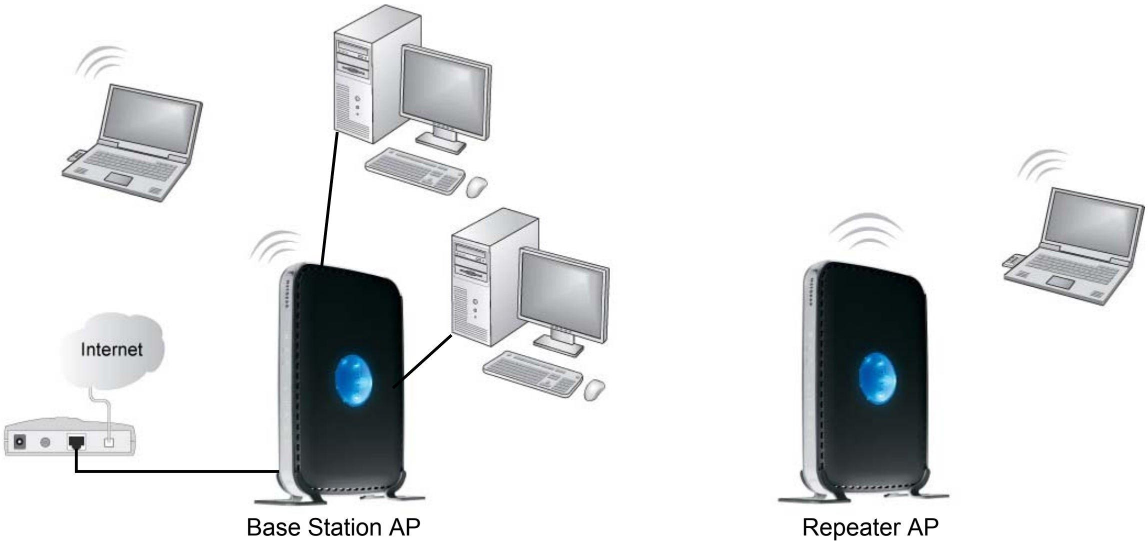


Figure 6-12

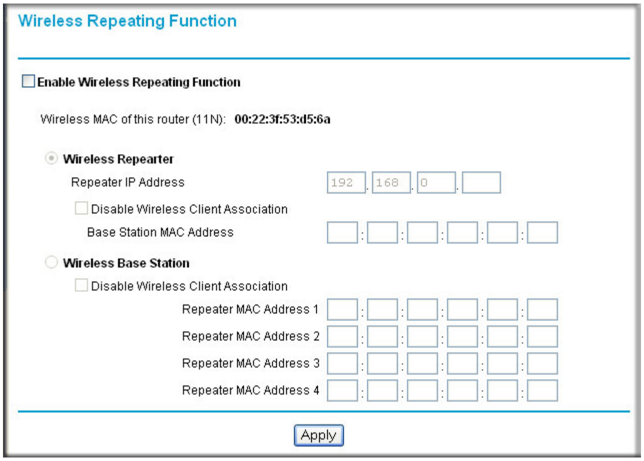
To set up a wireless network using WDS, the following conditions must be met for both APs:

- Both APs must use the same SSID, wireless channel, and encryption mode (see "Manually Configuring Your Wireless Settings" on page 2-4 or "Using Push 'N' Connect (WPS) to Configure Your Wireless Network" on page 2-10).
- Both APs must be on the same LAN IP subnet. That is, all the AP LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) must be configured to operate in the same LAN network address range as the APs.

- When the modem router is in dual band mode (the **Mode** field on the Wireless Settings screen is set to **Up to 270 Mbps at 5 GHz and 54 Mbps at 2.4 GHz**), the WDS function works only in 5GHz 11N mode. To use the 2.4GHz 11g protocol with WDS, set the **Mode** field in the Wireless Settings screen to **Up to 270 Mbps at 2.4 GHz**. If you make changes in the Wireless Settings screen, click **Apply** so that they take effect.

Wireless Repeating Function

You can view or change wireless repeater settings for the modem router. From the main menu of the browser interface, under Advanced, click **Wireless Repeating Function** to display the Wireless Repeating Function screen.



Wireless Repeating Function

☐ Enable Wireless Repeating Function

Wireless MAC of this router (11N): **00:22:3f:53:d5:6a**

● Wireless Repearter

Repeater IP Address 192 . 168 . 0 .

☐ Disable Wireless Client Association

Base Station MAC Address

○ Wireless Base Station

☐ Disable Wireless Client Association

Repeater MAC Address 1

Repeater MAC Address 2

Repeater MAC Address 3

Repeater MAC Address 4

Figure 6-13

The modem router supports two modes of the wireless repeating function, and allows you to control wireless client association:

- **Wireless Repeater**. The modem router sends all traffic from its local wireless or wired computers to a remote AP. To configure this mode, you must know the MAC address of the remote parent AP.
- **Wireless Base Station**. The modem router acts as the parent AP, bridging traffic to and from the child repeater AP, as well as handling wireless and wired local computers. To configure this mode, you must know the MAC addresses of the child repeater AP.
- **Disable Wireless Client Association**. Usually this check box is cleared so that the modem router is an access point for wireless computers.

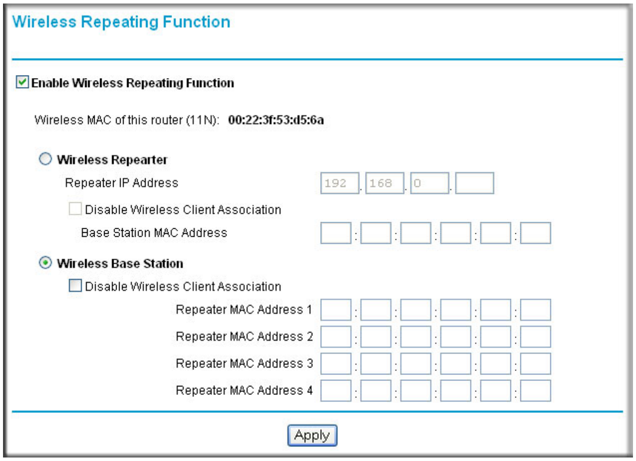
If this check box is selected, the modem router communicates wirelessly only with other APs whose MAC addresses are listed in this screen. The modem router still communicates with wire-connected LAN devices.

Setting Up the Base Station

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

To set up the base station:

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). Note that the wireless security option must be set to **None** or **WEP**.
2. Log into the modem router base unit, under the Advanced heading, select **Wireless Repeating Function** to display the Wireless Repeating Function screen.



Wireless Repeating Function

☑ Enable Wireless Repeating Function

Wireless MAC of this router (11N): 00:22:3f:53:d5:6a

○ Wireless Repearter

Repeater IP Address 192 . 168 . 0 .

□ Disable Wireless Client Association

Base Station MAC Address : : : : :

● Wireless Base Station

□ Disable Wireless Client Association

Repeater MAC Address 1 : : : : :

Repeater MAC Address 2 : : : : :

Repeater MAC Address 3 : : : : :

Repeater MAC Address 4 : : : : :

Figure 6-14

3. Select the **Enable Wireless Repeating Function** check box and the **Wireless Base Station** radio button.
4. Enter the MAC address for the repeater units.
5. Click **Apply** to save your changes.

Setting Up a Repeater Unit

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

> **Note:** If you are using the DGND3300 base station with a non-NETGEAR modem router as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

To configure a Dual Band Wireless-N Modem Router as a repeater unit:

1. If you are using the same model of modem router for both the base station and repeaters, you must change the LAN IP address for each repeater to a different IP address in the same subnet (see "Using the LAN Setup Options" on page 6-1).

   > **Note:** Failing to change the LAN IP address will cause an IP address conflict in the network because the factory default LAN IP is the same for both units.

2. Log in to the router that will be the repeater. Check the Wireless Settings screen, and verify that the wireless settings match the base unit exactly. The wireless security option must be set to **WEP** or **None**.
3. In the Wireless Repeating Function screen, select the **Enable Wireless Repeater Mode** radio button.

   This IP address must be in the same subnet as the base station but different from the LAN IP of the base station.
4. Fill in the **Base Station MAC Address** field.
5. Click **Apply** to save your changes.
6. Verify connectivity across the LANs.

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

Chapter 7
Fine-Tuning Your Network

This chapter describes features to help you manage your RangeMax Dual Band Wireless-N Modem Router.

This chapter includes the following sections:

Common connection types and their speed and security considerations are:

- **Broadband Internet**. Your Internet connection speed is determined by your modem type, (ADSL), as well as the connection speed of the sites to which you connect, and general Internet traffic. ADSL 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 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 modem router provides a wireless data throughput of up to 300 Mbps using technology called multiple input, multiple output (MIMO), in which multiple antennas transmit multiple streams of data. The use of multiple antennas also provides excellent range and coverage. 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 for your computers. Although your modem 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. Table 7-1 shows the time to transfer 1 gigabyte (GB) of data using various networking technologies.

Table 7-1. 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)

Optimizing Your Network Bandwidth

As your network grows, it might consist of several segments of different networking technologies, each providing different throughput. In planning your network, you should first consider which devices will have the heaviest traffic flow between them. Examples are:

- A media center in one room streaming high-definition video from a server in another room
- A storage device that is used for backing up your computers

Next, consider the throughput of your network devices. Where possible, make the heaviest-traffic connections using higher-speed technologies, with no lower-speed bottlenecks in the path.

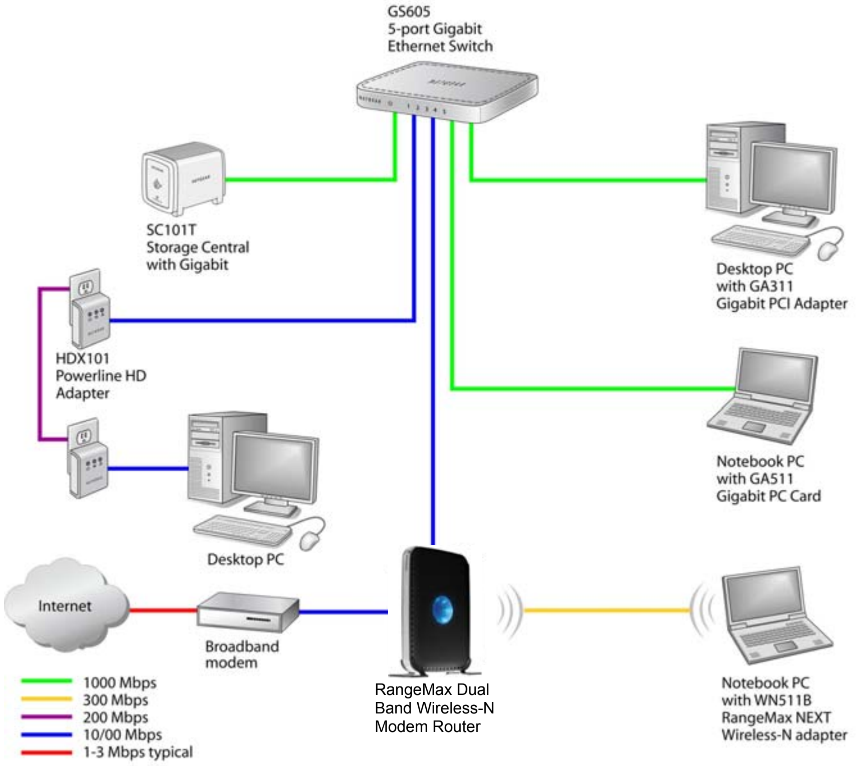


Figure 7-1

Figure 7-1 shows a sample network using multiple networking technologies. In this network, the two PCs with Gigabit (1000 Mbps) Ethernet adapters have a gigabit connection through the GS605 switch to the storage server. This connection should allow for extremely fast backups or quick access to large files on the server. The PC connected through a pair of Powerline HD adapters is limited to the 200 Mbps speed of the Powerline HD connection. Although any of the links in this example would be sufficient for high-traffic applications such as streaming HD video, the use of older devices such as 10 Mbps Ethernet or 802.11b wireless would create a significant bottleneck.

Optimizing Wireless Performance

The speed and operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless router. You should choose a location for your router that will maximize the network speed.

➡	**Note:** Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range and performance specifications, click the link to the online document "Wireless Networking Basics" in Appendix B.

The following list describes how to optimize wireless router performance.

- **Identify critical wireless links.**
  If your network has several wireless devices, decide which wireless devices need the highest data rate, and locate the router near them. Many wireless products have automatic data-rate fallback, which allows increased distances without loss of connectivity. This also means that devices that are farther away might be slower. Therefore, the most critical links in your network are those where the traffic is high and the distances are great. Optimize those first.
- **Choose placement carefully.**
  For best results, place your router:
  - Near the center of the area in which your computers will operate.
  - In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
  - Avoid obstacles to wireless signals.
  - Keep wireless devices at least 2 feet from large metal fixtures such as file cabinets, refrigerators, pipes, metal ceilings, reinforced concrete, and metal partitions.
  - Keep away from large amounts of water such as fish tanks and water coolers.
- **Reduce interference.**
  - Avoid windows unless communicating between buildings.
  - Place wireless devices away from various electromagnetic noise sources, especially those in the 2400–2500 MHz frequency band. Common noise-creating sources are:
    - Computers and fax machines (no closer than 1 foot)
    - Copying machines, elevators, and cell phones (no closer than 6 feet)

  - Microwave ovens (no closer than 10 feet)
- **Choose your settings.**
  - Use a scanning utility to determine what other wireless networks are operating nearby, and choose an unused channel.
  - Turn off SSID broadcast, and change the default SSID. Other nearby devices might automatically try to connect to your network several times a second, which can cause significant performance reduction.
- Use WMM to improve the performance of voice and video traffic over the wireless link.

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 the technical support of either the ISP or NETGEAR recommends changing the MTU setting. These might require an MTU change:
  - A secure website that won’t open, or displays only part of a Web page
  - Yahoo e-mail
  - 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 to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500 until the problem goes away. Table 7-2 describes common MTU sizes and applications.

Table 7-2. Common MTU Sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This is the typical setting for non-PPPoE, non-VPN connections, and is the default value for NETGEAR routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1460	Usable by AOL if you don't 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.

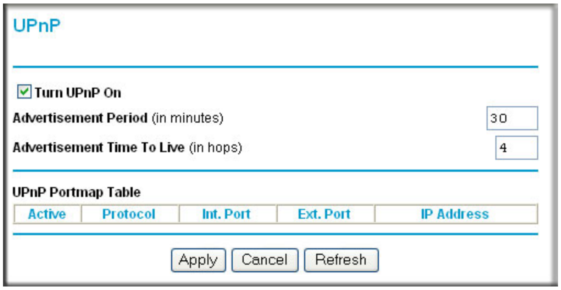
Universal Plug and Play

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. From the main menu, under Advanced, click **UPnP**. The UPnP screen displays.



UPnP

☑ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time To Live (in hops) 4

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

Figure 7-2

2. The available settings and information in this screen are:
   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If this check box is not selected, the router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.
   - **Advertisement Period**. The advertisement period is how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations 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.

Chapter 8
Troubleshooting

This chapter provides information about troubleshooting your RangeMax Dual Band Wireless-N Modem 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 firmware updates at *http://www.netgear.com/support*.

This chapter includes the following sections:

- Quick Tips
- "Troubleshooting with the LEDs" on page 8-2
- "Cannot Access the Internet" on page 8-5
- "Troubleshooting a Network Using the Ping Utility" on page 8-7
- "Problems with Date and Time" on page 8-9
- "Wireless Connectivity" on page 8-9

Quick Tips

This section describes tips for troubleshooting some common problems.

Table 8-1. Quick Tips

Recommendation	Instructions
You can turn off the dome lights for the modem router.	Tap the dome to turn off the lights. These lights identify the activity of the eight internal antennas, flashing to show which combination of antennas is receiving the strongest signals.
Be sure to restart your network in this sequence.	1. Unplug the modem router. 1. Turn off the computers. 2. Plug in the modem router. Wait 1 minute. 3. Turn on the computers.

Table 8-1. Quick Tips (continued)

Recommendation	Instructions
Make sure that the Ethernet cables are securely plugged in.	For each powered-on computer connected to the modem router by an Ethernet cable, the corresponding numbered router LAN port LED 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 wireless security settings of the modem routerand wireless computer must match exactly. • If you set up an Access List in the Advanced Wireless Settings screen, you must add each wireless computer's MAC address to the modem router's access list.
Make sure that the network settings of the computer are correct.	• Wired and wirelessly connected computers *must* have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP. Click the link to the online document "Preparing Your Network" in Appendix B, or see the documentation that came with your computer. • Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the Attached Devices screen.
Check the Test LED to verify correct modem router operation.	If the Test LED does not turn off within 2 minutes after you turn the modem router on, reset the router according to the instructions in "Using the Restore Factory Settings Button" on page A-1.

Troubleshooting with the LEDs

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

1. When power is first applied, verify that the Power LED ⏻ is on.
2. After approximately 10 seconds, verify that:
   - The Power LED is green.
   - The LAN port LEDs are lit for any local ports that are connected. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be amber.
   - The ADSL link LED is lit, indicating that a link has been established to the connected device.

- The Wireless LEDs are lit.

If any of the above conditions does not occur, see the following table.

Table 8-2. Troubleshooting with the LEDs

Situation	Recommended Action
Power LED is off.	If the Power and other LEDs are off when your router is turned on: • Make sure that the power cord is properly connected to your router and that the power supply 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.
Power LED is red. The power LED turns red when you depress the Restore Factory Settings button, and blinks red 3 times when that button is released. This is normal and does not indicate a problem.	If the Power LED remains red, there is a fault within the router. • Cycle the power to see if the router recovers. • Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Restoring the Factory Configuration Settings" in Appendix A. If the error persists, you might have a hardware problem and should contact technical support.
LEDs never turn off.	When the router is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the router. If all LEDs are still on 1 minute after power up: • Cycle the power to see if the router recovers. • Clear the router's configuration to factory defaults as explained in "Restoring the Factory Configuration Settings" in Appendix A. If the error persists, you might have a hardware problem and should contact Technical Support at *www.netgear.com/support*.
ADSL Link LED is off.	• Disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones. • Check that the telephone company has made the connection to your line and tested it. • Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It may be necessary to use a swapper if your ADSL signal is on pins 1 and 4 of the RJ-11 jack. The Dual Band Wireless-N Modem Router uses pins 2 and 3.
Internet LED is red.	The modem router cannot access the Internet. See "Cannot Access the Internet" on page 8-5.

Table 8-2. Troubleshooting with the LEDs

Situation	Recommended Action
The Ethernet port LEDs are off.	If the Ethernet port LEDs do not light when the Ethernet connection is made, check the following: • Make sure that the Ethernet cable connections are secure at the modem router and computer. • Make sure that power is turned on to the connected modem or computer.
Wireless LEDs are off.	If the Wireless LEDs do not come on, verify that the **Enable Wireless Router Radio** check box is selected in the Advanced Wireless Settings screen. See "Advanced Wireless Settings" on page 2-15.

Cannot Access the Modem Router Menu

If you are unable to access the router's menu from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the modem router.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to "Preparing Your Network" in Appendix B to find your computer's IP address.
- If your computer's IP address is shown as 169.254.x.x:, it might because recent versions of Windows and MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Restoring the Factory Configuration 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 quitting the browser and launching it again.
- Make sure you are using the correct login information. The login name is **admin** and the default password is **password**. Make sure that Caps Lock is off when entering this information.

If the modem router does not save changes you have made in the modem router menu, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another screen, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Cannot Access the Internet

➡	**Note:** If you are installing the modem router and have not yet configured the Internet connection, see Chapter 1, “Configuring Your Internet Connection” or the *Setup Manual*.

If your Internet connection was working previously, it is possible that this is due to a problem at your ISP. If you can access your router but you are unable to access the Internet, you can check its configuration, and you can determine whether the router can obtain an IP address from your Internet Service Provider (ISP).

Checking the Configuration

To check the router configuration to make sure that it is correct:

1. Start your browser, and select an external site such as *http://www.netgear.com*.
2. Access the main menu of the router at *http://www.routerlogin.net*.
   - Select Basic Settings to view the Basic Settings screen.
   - Select ADSL to view the settings for Multiplexing method, VPI, and VCI settings.
   - You can select Setup Wizard and allow the modem router to automatically detect your Internet connection.

Checking the WAN IP Address

Unless your ISP provides a fixed IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Router Status screen.

To check the WAN IP address:

1. Start your browser, and select an external site such as *http://www.netgear.com*.

2. Access the main menu of the router at *http://www.routerlogin.net*.
3. Under Maintenance, select **Router Status**.
4. Check that an IP address is shown for the Internet port. If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by restarting your network, as described in Table 8-1 on page 8-1.

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

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

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

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically, your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer, and verify the DNS address as described in the online document you can access from "Preparing Your Network" in Appendix B. You can also configure your computer manually with DNS addresses, as explained in your operating system documentation.
- Your computer might not have the router configured as its TCP/IP gateway.

  If your computer obtains its information from the router by DHCP, reboot the computer, and verify the gateway address as described in the online document you can access from "Preparing Your Network" in Appendix B.

- 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 modem router. You might need to go to Internet Explorer and select **Tools** > **Internet Options**, click the Connections tab, and select **Never dial a connection**.

Troubleshooting a Network Using the Ping Utility

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

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 the Start button, 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 the numbered Ethernet port LED is on for the port to which you are connected. If the LED is off, follow the instructions in Table 8-2 on page 8-3.

  - Check that the corresponding Link LEDs are on for your network interface card. If your router and computer are connected to a separate Ethernet switch, make sure the Link LEDs are on for the switch ports that are connected to your computer and router.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
  - Verify that the IP address for your router and your computer are correct and that the addresses are on the same subnet.

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 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

Under Security in the main menu, select Schedule to view the current date and time of day. The modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

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

Wireless Connectivity

Note: If you are installing the modem router and have not yet set up a wireless connection, see Chapter 2, "Safeguarding Your Network"or the *Setup Manual*.

To add a wireless computer to an existing wireless network, you must set up its wireless card to match the modem router's settings. You can use Push 'N' Connect (WPS) ("Connecting Additional Wireless Client Devices After WPS Setup" on page 2-14) if your computer supports it. You can also manually configure the computer's wireless settings.

When you install a NETGEAR wireless card in your computer, a Smart Wizard 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.

If you have no specific wireless card setup program installed, you can use the basic setup utility in Windows by following these steps:

1. Open the Windows Control Panel, and double-click **Network Connections**.
2. In the LAN section, double-click **Wireless Network Connection**.

Viewing Available Networks

If your wireless computer is configured for the network, but you cannot connect, use the computer's wireless setup program to scan for available wireless networks. Look for network names (SSIDs) of **NETGEAR-DualBand-N** and **NETGEAR-2.4-G**, or your custom SSIDs if you have changed them. If your wireless networks do not appear, check these conditions:

- Is your modem router's wireless radio enabled? See "Advanced Wireless Settings" on page 2-15.
- Is your modem router's SSID broadcast enabled? See "Advanced Wireless Settings" on page 2-15
- Is your modem router set to a wireless standard that is not supported by your wireless card? Check the Mode setting, as described in "Manually Configuring Your Wireless Settings" on page 2-4.

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

- Is your modem router too far from your computer, or too close? Place your computer near the router, but at least 6 feet away, and see whether the signal strength improves.
- Is your wireless signal obstructed by objects between the router and your computer? See "Wireless Placement and Range Guidelines" on page 2-2.

If your wireless network appears and has good signal strength:

- Is your modem router using the same channel as other nearby wireless networks? If this is the case, there might be interference from other wireless networks. You can change the channel in the Wireless Settings screen. See "Manually Configuring Your Wireless Settings" on page 2-4.
- Test another wireless device to see if the problem is limited to a specific computer.
- You can also disable the modem router's wireless security while testing to help isolate the problem.

Appendix A
Default Configuration and Technical Specifications

This appendix provides factory default settings and technical specifications for the RangeMax Dual Band Wireless-N Modem Router.

Restoring the Factory Configuration Settings

> **Note:** This procedure erases your current configuration, including your wireless security. When you log in after resetting, you will be prompted to configure these settings.

This section explains how to restore the factory default configuration settings. This procedure restores the **admin** user name password to **password,** and the IP address to **192.168.0.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see “Erasing the Configuration” on page 4-10).
- 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.

Using the Restore Factory Settings Button

To restore the factory configuration settings without knowing the administration password or IP address, you must use the Restore Factory Settings button on the rear panel of the modem router.

1. Press and hold the Restore Factory Settings button until the Power LED turns red (about 6 seconds).
2. Release the Restore Factory Settings button and wait for the router to reboot.The Power LED will blink red three times and then will turn green when the default configuration settings have been restored.

Table A-1. Default Configuration Settings

Feature		Default Setting
Router login		
	Modem Router login URL	http://www.routerlogin.net *or* http://www.routerlogin.com
	User name (case-sensitive)	admin
	Password (case-sensitive)	password
	USB access	\\readyshare
Internet connection		
	WAN MAC address	Use default address
	WAN MTU size	1458 for Annex A World except NA, 1492 for Annex A NA and Annex B
	ADSL line rate	automatically negotiated
Local network (LAN)		
	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Disabled
	Time zone	GMT for Annex A except NA ; PST for NA; GMT + 1 H for Annex B.
	Time zone adjusted for daylight saving time	Disabled
	SNMP	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Table A-1. Default Configuration Settings (continued)

Feature		Default Setting
Wireless		
	Wireless communication	Enabled
	Name (11N SSID)	NETGEAR-Dual Band-N
	Name (11G SSID)	NETGEAR-2.4G
	Security	Disabled
	Broadcast SSID	Enabled
	Country/Region	United States in North America, otherwise varies by region. For Annex B, Germany is default region.
	11N Channel	36/5.180GHz
	11G Channel	Auto*
	Operating Mode	Up to 270Mbps at 5GHz and 54Mbps at 2.4GHz
	Output Power	Full

*. Maximum Wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.

Technical Specifications

Table A-1. Specifications

Feature		General
Network Protocol and Standards Compatibility		
Data and Routing Protocols		TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power Adapter		
	North America	120V, 60 Hz, input
	UK, Australia	240V, 50 Hz, input
	Europe	230V, 50 Hz, input
	All regions (output)	12V @ 1.5A output
Physical		
	Dimensions	8.9" x 6.8" x 1.5" (225.5 mm x 172 mm x 39 mm)
	Weight	1.2 lbs. (0.54 kg)

Table A-1. Specifications (continued)

Environmental		
	Operating temperature	0° to 40° C (32º to 104º F)
	Operating humidity	10% to 90% relative humidity, noncondensing
	Storage temperature	-20° to 70° C (-4º to 158º F)
Regulatory Compliance		
	Meets requirements of	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
Interface Specifications		
	LAN	10BASE-T or 100BASE-Tx, RJ-45
	WAN (ADSL)	ITU 992.1 (G.dmt) Annex A, ITU 992.2 (G.lite), ITU 992.3 ADSL2 (G.dmt.bis), ITU 992.5 ADSL2+. Annex A ADSL is supported by DGND3300, Annex B ADSL is supported by DGND3300.
USB		
	File systems	FAT, FAT32, NTFS (read only) and Linux

Appendix B
Related Documents

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
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 Basics	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

In addition, you can find initial setup instructions for your modem router in the *Setup Manual*.

Index