DG834N RangeMax NEXT Wireless ADSL2+ Modem Router Reference Manual

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

202-10197-01
May 2006

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks 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.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

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 generates, 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 measures:

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

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

European Union Statement of Compliance

Hereby, NETGEAR, Inc. declares that this wireless modem router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Èesky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router 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 DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router 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 DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router 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 DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router 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 DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarç, ka DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router 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 DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oœwiadcza, ¿e DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the DG834N product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das DG834N RangeMax™ NEXT Wireless ADSL2+ 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.

Certificate of the Manufacturer/Importer

It is hereby certified that the DG834N RangeMax™ NEXT Wireless ADSL2+ 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.

Voluntary Control Council for Interference (VCCI) Statement

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

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router.

World Wide Web

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) *http://www.netgear.com*. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

Product and Publication Details

Model Number:	DG834N
Publication Date:	May 2006
Product Family:	Wireless Modem Router
Product Name:	DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10197-01
Publication Version Number:	1.0

Contents

DG834N RangeMax NEXT Wireless ADSL2+ Modem Router Reference Manual

Chapter 1
Introduction

Chapter 2
Configuring Your Internet Connection

Chapter 3
Wireless Configuration

Chapter 4
Protecting Your Network

Chapter 5
Managing Your Network

Chapter 6
Advanced Configuration

About This Manual

The *NETGEAR® DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router Reference Manual* describes how to install, configure and troubleshoot the DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router.The information is this manual is intended for readers with 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::

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text, file and server names, extensions, commands, IP addresses

- **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 may result in a malfunction or damage to the equipment.

Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the RangeMax NEXT Wireless ADSL2+ Modem Router according to these specifications:

Product Version	DG834N RangeMaxTM NEXT Wireless ADSL2+ Modem Router
Manual Publication Date	May 2006

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

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com/products/DG834N.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A button that displays the table of contents and an button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View**.

Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter**.

  Use the *PDF of This Chapter* link at the top left of any page.

  – Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

  – Your computer must have 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*.

  – Click the print icon in the upper left of the window.

> **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.

- **Printing the Full Manual**.

  Use the *Complete PDF Manual* link at the top left of any page.

  – Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

  – Click the print icon in the upper left of the window.

> **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.

Chapter 1
Introduction

This chapter lists the items that come with the NETGEAR DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router, and describes the front and rear panels.

What's in the Box?

The product package should contain the following items:

- DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router
- Plastic base for standing the unit upright
- AC power adapter (varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable
- Microfilters (quantity and type vary by region)
- *Resource CD*, which includes this guide
- Warranty and Support Information cards

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

The Router's Front Panel

The DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router front panel shown below contains status LEDs.

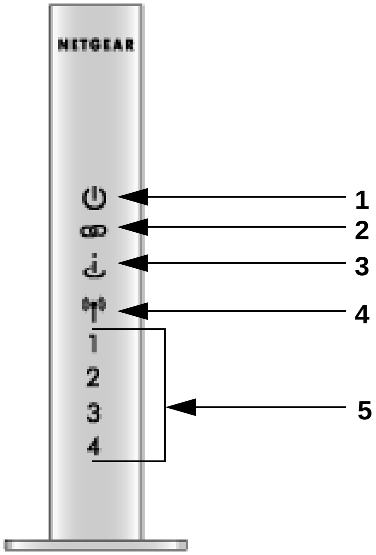


Figure 1-1

You can use the LEDs to verify various conditions. Table 1-1 lists and describes each LED on the front panel of the router.

Table 1-1. LED Descriptions

Item	Function	Activity	Description
1	Power	On (green) Blink (green) Solid On (red) Brief On (red) Off	Power is supplied to the router. Firmware upgrade is in progress Power On Self Test failure or device malfunction. Lights red when the reset button is depressed for 5 seconds, which resets the unit to factory default settings. Blinks red three times when the button is released. Power is not supplied to the router.
2	PPP Link	On (green) Blinking Off	There is an Internet session. If the session is dropped due to an idle timeout, and an ADSL connection is still present, the light will remain green. If the session is dropped for any other reason, the light will turn off. IP traffic is passing through the wireless modem router. The unit is off or there is no IP connection.

Table 1-1. LED Descriptions (continued)

3	Internet (WAN)	On (green) Blink (green) Blink (amber) Off	The ADSL port is synchronized with an ISP's network-access device. Data is being transmitted over the ADSL port. Indicates ADSL training. No connection detected on the ADSL port.
4	Wireless	On Blink Off	Indicates that the Wireless port is initialized. Data is being transmitted or received over the wireless link. The Wireless Access Point is turned off.
5	LAN	On (green) Blink (green) On (amber) Blink (amber) Off	The Local port has detected a link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected a link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected on this port.

The Router's Rear Panel

The rear panel of the DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router (Figure 1-2) contains port connections.

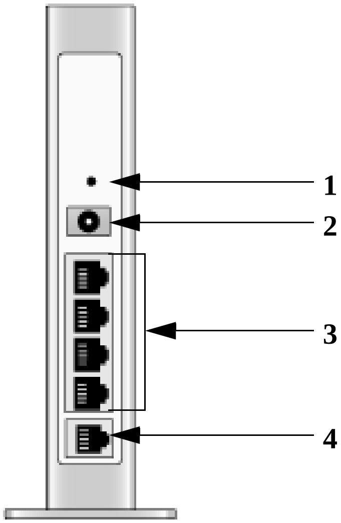


Figure 1-2

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

1. Factory Default Reset push button

➡	**Note:** This button needs to be depressed for approximately 5 seconds, until the power LED briefly flashes red, to reset the unit to the factory default settings.

2. DC power in
3. Four Local Ethernet RJ-45 LAN ports for connecting the router to the local computers
4. RJ-11 ADSL port for connecting the router to an ADSL line

Chapter 2
Configuring Your Internet Connection

This chapter describes how to configure the wired internet connection of your DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router.

Connecting the Router to the Internet

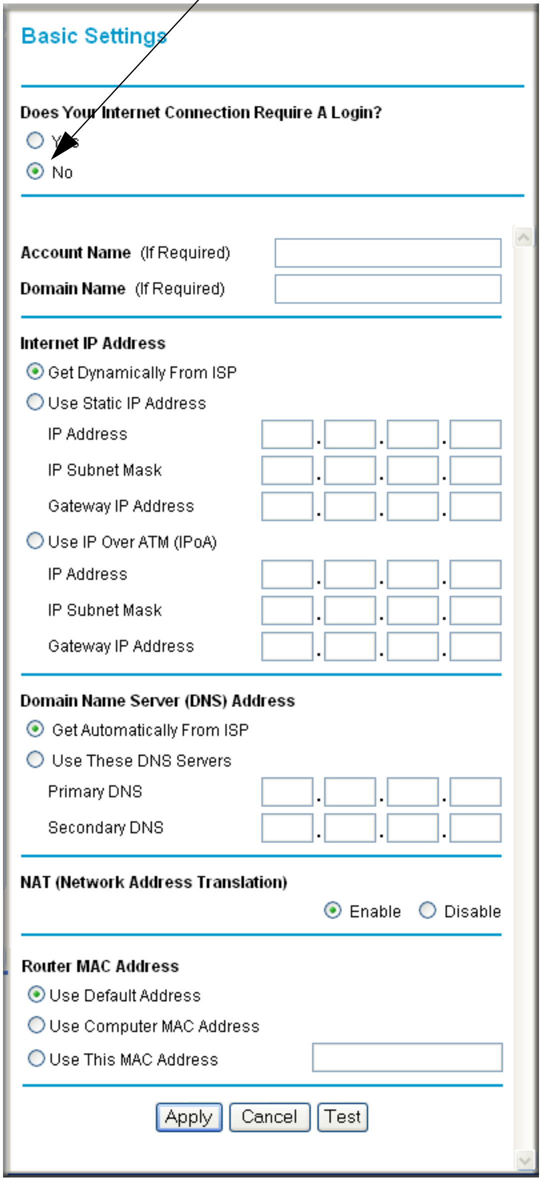
To connect your RangeMax NEXT Wireless ADSL2+ Modem Router to the Internet, refer to the *ADSL Modem Wireless Router Setup Manual* on the *Resource CD* or online as shown in the following table.

Table 2-1.

Language	**URL**
Dutch	*http://documentation.netgear.com/dg834n/nld/208-10092-01/*
English	*http://documentation.netgear.com/dg834n/enu/208-10087-01/*
French	*http://documentation.netgear.com/dg834n/fra/208-10090-01/*
German	*http://documentation.netgear.com/dg834n/deu/208-10088-01/*
Italian	*http://documentation.netgear.com/dg834n/ita/208-10091-01/*
Spanish	*http://documentation.netgear.com/dg834n/esp/208-10089-01/*
Swedish	*http://documentation.netgear.com/dg834n/sve/208-10093-01/*

How to Manually Configure Your Internet Connection

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

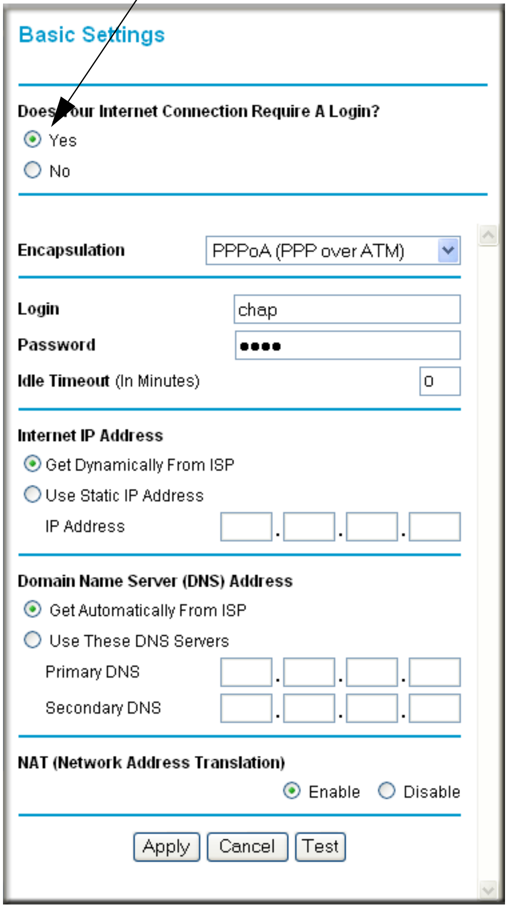
NAT (Network Address Translation)

● Enable ○ Disable

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: chap

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

Figure 2-1

You can manually configure the router using the Basic Settings menu shown in Figure 2-1 using these steps:

1. Connect to the wireless modem router by typing *http://www.routerlogin.net* in the address field of your browser, then click **Enter**.
2. For security reasons, the wireless modem router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters.
3. Click **Basic Settings** in the Setup section of the main menu.
4. If your Internet connection does not require a login, click **No** at the top of the Basic Settings menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click **Yes**, and skip to step 5.

   a. Account Name (may also be called Host Name) and Domain Name: These parameters may be necessary to access your ISP's services such as mail or news servers.

   b. Internet IP Address:

   If you log in to your service or your ISP did not provide you with a fixed IP address, select **Get Dynamically From ISP**. With this option, the router will find an IP address for you automatically when you connect.

   If your ISP has assigned you a permanent, fixed (static) IP address for your computer, select **Use Static IP Address**. Enter the IP address that your ISP assigned. Also enter the net mask and the Gateway IP address. The Gateway is the ISP's router to which your router will connect.

   If your ISP uses classical or routed IP Over ATM (Internet Protocol over Asynchronous Transfer Mode switched virtual circuits) select **Use IP Over ATM (IPoA)**. Enter the IP address, subnet address and gateway IP address provided by your ISP in the appropriate text boxes.

   c. Domain Name Server (DNS) Address:
   If you know that your ISP does not automatically transmit DNS addresses to the router during login, select **Use These DNS Servers** and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

   ➡ **Note:** If you enter an address here, restart the computers on your network so that these settings take effect.

d. NAT (Network Address Translation): Allows all the PCs connected to your router to gain Internet access by sharing the router’s WAN IP address. In most cases, NAT is essential for Internet access via this wireless modem router. Only select **Disable** if you are sure you do not require NAT. When disabled, only standard IP routing is performed.

e. Router’s MAC Address:
This section determines the Ethernet MAC address that will the router will use on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by “cloning” its MAC address.

To change the MAC address, select **Use Computer MAC Address**. The router will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. Or, select **Use this MAC address** and type it in here.

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

5. If your Internet connection does require a login, fill in the settings according to the instructions below. Select **Yes** if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.

> **Note:** After you finish setting up your router, you will no longer need to launch the ISP’s login program on your computer in order to access the Internet. When you start an Internet application, your router will automatically log you in.

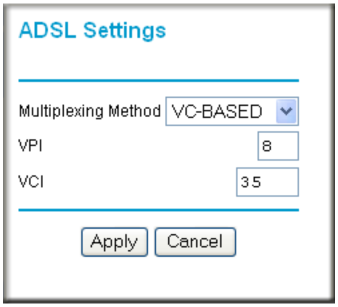
a. Select the protocol used by your ISP from the **Encapsulation** drop-down list. PPPoE is the most common option.

b. The screen will change according to the ISP settings requirements of the ISP you select.

c. Fill in the parameters for your Internet service provider.

d. Click **Apply** to save your settings. Click the **Test** button to verify you have Internet access.

6. If your ISP provided information about multiplexing and/or VPI and VCI settings for you to enter, click the **ADSL Settings** in the Setup section of the main menu. Usually, however, the default parameters will match the system used by your ISP



ADSL Settings

Multiplexing Method: VC-BASED

VPI: 8

VCI: 35

Figure 2-2

Chapter 3
Wireless Configuration

This chapter describes how to configure the wireless features of your DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router.

Considerations for a Wireless Network

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your wireless modem router in order to maximize the network speed. For further information, refer to "Internet Networking and TCP/IP Addressing:" in Appendix B.

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

Observe Performance, Placement, and Range Guidelines

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

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range/performance specifications, please see Appendix A, "Technical Specifications".

For best results, place your firewall:

- 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)
- Away from sources of interference, such as computers, microwaves, and cordless phones
- Away from large metal surfaces

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.

Implement Appropriate Wireless Security

> **Note:** Indoors, computers can connect over wireless networks at a range of several hundred feet. Such distances can allow for others outside of 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 RangeMax NEXT Wireless ADSL2+ Modem Router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

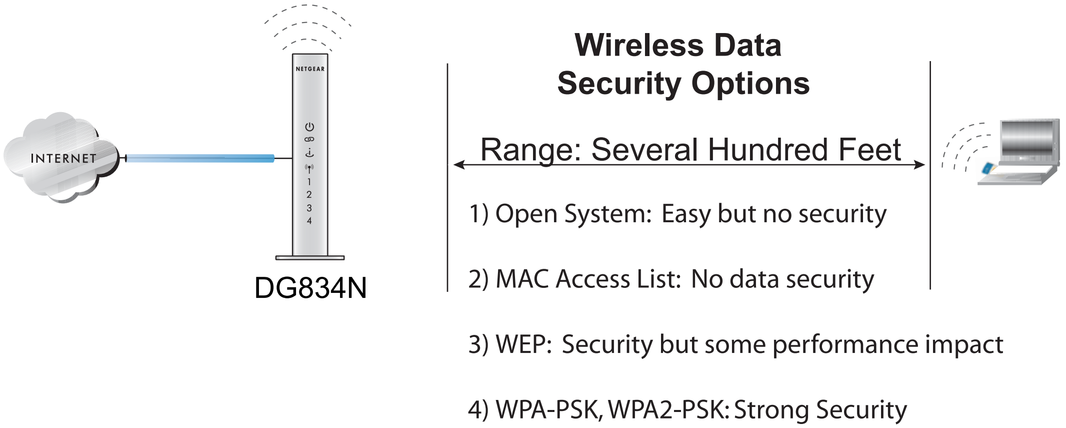

INTERNET
NETGEAR
DG834N
Wireless Data
Security Options
Range: Several Hundred Feet
1) Open System: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but some performance impact
4) WPA-PSK, WPA2-PSK: Strong Security

Figure 3-1

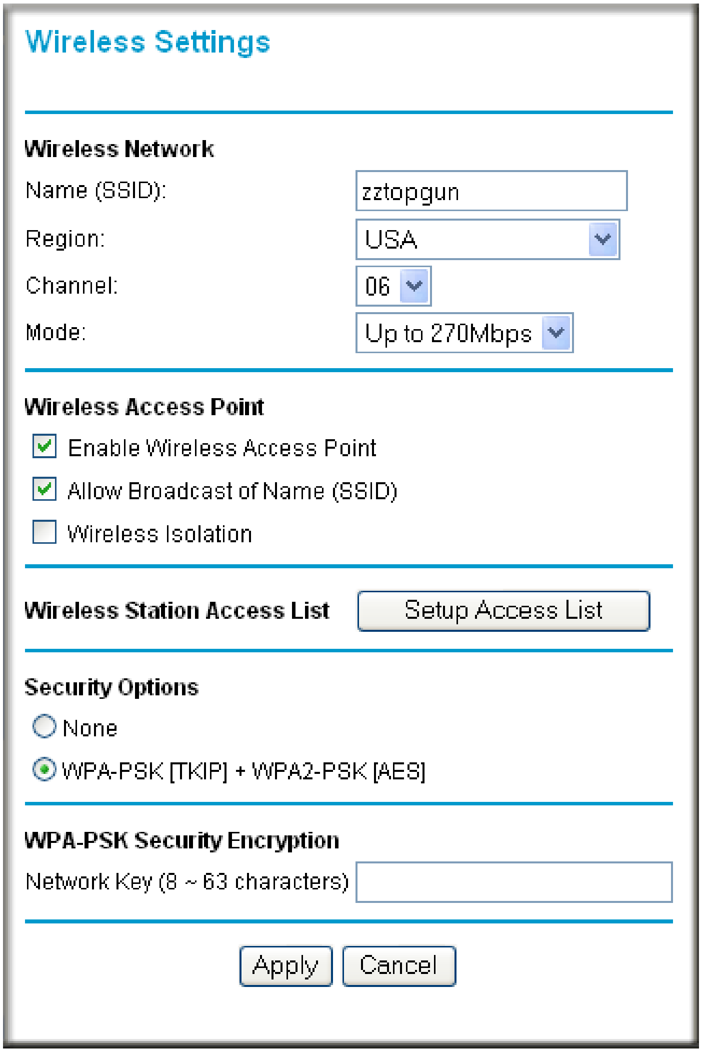
There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC Address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the DG834N. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network ‘discovery’ feature of some products, such as Windows XP, but the data is still exposed.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK, and is only available as an option if the Wireless Mode is restricted to 802.11b and 802.11g wireless stations.
- **WPA-802.1x, WPA2-802.1x.** Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and RADIUS servers. This option is only available if the Wireless Mode is restricted to 802.11b and 802.11g wireless stations.
- **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 make it virtually impossible to compromise. Because this is a relatively new standard, wireless device driver and software availability may be limited. This is the recommended mode, and is the only one available in the fastest “Up to 130 Mbps” and “Up to 270 Mbps” wireless network modes.

Understanding Wireless Settings

To configure the Wireless interface of your wireless modem router, click the Wireless link in the main menu of the browser interface. The following Wireless Settings menu will appear:



Wireless Settings

Wireless Network

Name (SSID): zztopgun

Region: USA

Channel: 06

Mode: Up to 270Mbps

Wireless Access Point

☑ Enable Wireless Access Point

☑ Allow Broadcast of Name (SSID)

☐ Wireless Isolation

Wireless Station Access List

Security Options

○ None

● WPA-PSK [TKIP] + WPA2-PSK [AES]

WPA-PSK Security Encryption

Network Key (8 ~ 63 characters)

Figure 3-2

The following parameters are in the Wireless Settings menu:

Wireless Network.

- **Name (SSID)**. The Service Set ID, also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is **NETGEAR**, but NETGEAR strongly recommends that you change your network Name to a different value.

  This value is case sensitive. For example, **Wireless** is not the same as **wireless**.

- **Region**. Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the wireless modem router in a region other than the region shown here.

- **Channel**. This field determines which operating frequency will be used. If you select the AUTO setting, the RangeMax NEXT Wireless ADSL2+ Modem Router will periodically survey the wireless environment to ensure that it is using the clearest channel. If a clearer channel is available, it may automatically switch channels.

> **Note:** After the router switches channels, there may be a slight delay while your wireless computers reconnect to the router. If you want to avoid this possibility, leave channel selection on a fixed channel setting.

- **Mode**.

  — “Up to 270Mbps” means all 802.11g, 802.11b, and faster Draft-N wireless stations can be used. This mode expands the channel bandwidth from 20 MHz to 40 MHz to achieve the 270 Mbps rate. The router selects channel expansion on a frame-by-frame basis to avoid interference with the data transmissions of other access points or wireless stations. This mode is the fastest mode and, since it is compatible with older wireless stations, it is recommended and is the default.

  — “Up to 130Mbps” allows wireless stations that support speeds up to 130 Mbps. In this case, the router will transmit two streams with different data concurrently on the same channel. You may want to select this mode to restrict channel bandwidth in order to minimize interference with the data transmissions of other access points and wireless stations.

  — "g & b" allows older 802.11g and 802.11b wireless stations to access this device. You may want to select this mode if you have a wireless station that is using WEP security and does not support WPA-PSK or WPA2-PSK.

Wireless Access Point.

- **Enable Wireless Access Point**. This field lets you turn off or turn on the wireless access point built in to the wireless modem router. The wireless icon on the front of the wireless modem router will display the current status of the Wireless Access Point to let you know if it is disabled or enabled. The wireless access point must be enabled to allow wireless stations to access the Internet.
- **Allow Broadcast of Name (SSID)**. If enabled, the SSID is broadcast to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.
- **Wireless Isolation.** If enabled, Wireless Stations will not be able to communicate with each other or with Stations on the wired network. This feature should normally be disabled.

Wireless Station Access List.

- By default, any wireless computer that is configured with the correct wireless network name or SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only specific computers based on their MAC addresses. Click Setup Access List to display the Wireless Station Access List menu.

Security Options

Table 3-1. Wireless Security Options

Field	Description
None	Wireless security is not used.
WPA-PSK (TKIP) + WPA2-PSK (AES)	WPA Pre-Shared-Key (Wi-Fi Protected Access Pre-Shared Key) uses a pre-shared key to perform the authentication and generate the initial data encryption keys. .Then, it dynamically varies the encryption key. WPA-PSK (TKIP) implements most of the IEEE 802.11i standard and is designed to work with all wireless network interface cards, but not all wireless access points. WPA2 implements the full standard, but will not work with some older network cards. For a full explanation of WPA, see "Preparing a Computer for Network Access:" in Appendix B.
WEP (Wired Equivalent Privacy)	This mode is only available if the "g and b" wireless mode is selected. This mode has been superseded by WPA-PSK and WPA2-PSK, which should be selected if possible.
WPA-802.1x	User authentication is implemented using 802.1x and RADIUS servers. For a full explanation of WPA, see "Preparing a Computer for Network Access:" in Appendix B. This type of authentication is only available if the "g and b" wireless mode is selected.

How to Set Up and Test Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in to the DG834N firewall 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. Click the Wireless Settings link in the main menu of the DG834N wireless modem router.
3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is **NETGEAR**.

➡	**Note:** The SSID of any wireless access adapters must match the SSID you configure in the DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router. If they do not match, you will not get a wireless connection.

4. Set the Region. Select the region in which the wireless interface will operate.
5. Set the Channel if necessary. The default channel is 6.

   This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless modem router. If you set the channel to **Auto** the wireless modem router will find the clearest channel for you. However, if that channel becomes noisy, there may be a delay in wireless communications while the wireless modem router searches for a new channel. For more information on the wireless channel frequencies please refer to "Preparing a Computer for Network Access:" in Appendix B.
6. For initial configuration and test, leave the Wireless Card Access List set to allow everyone access by making sure that "Turn Access Control On" is not selected in the Wireless Station Access List. In addition, leave the Encryption Strength set to "None".
7. Click **Apply** to save your changes.

➡	**Note:** If you are configuring the firewall from a wireless computer and you change the firewall's SSID, channel, or security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the firewall's new settings.

8. Configure and test your computers for wireless connectivity.

Program the wireless adapter of your computers to have the same SSID and channel that you configured in the router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the wireless modem router.

Once your computers have basic wireless connectivity to the wireless modem router, you can configure the advanced wireless security functions of the firewall.

Restricting Wireless Access to Your Network

By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, the DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router provides several ways to restrict wireless access to your network:

- Turn off wireless connectivity completely
- Restrict access based on the Wireless Network Name (SSID)
- Restrict access based on the Wireless Card Access List

These options are discussed below.

Restricting Access to Your Network by Turning Off Wireless Connectivity

You can completely turn off the wireless portion of the DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router. For example, if your notebook computer is used to wirelessly connect to your router and you take a business trip, you can turn off the wireless portion of the router while you are traveling. Other members of your household who use computers connected to the router via Ethernet cables will still be able to use the router.

Restricting Wireless Access Based on the Wireless Network Name (SSID)

The DG834N can restrict wireless access to your network by not broadcasting the wireless network name (SSID). However, by default, this feature is turned off. If you turn this feature on, wireless devices will not ‘see’ your wireless modem router. You must configure your wireless devices to match the wireless network name (SSID) you configure in the RangeMax NEXT Wireless ADSL2+ Modem Router.

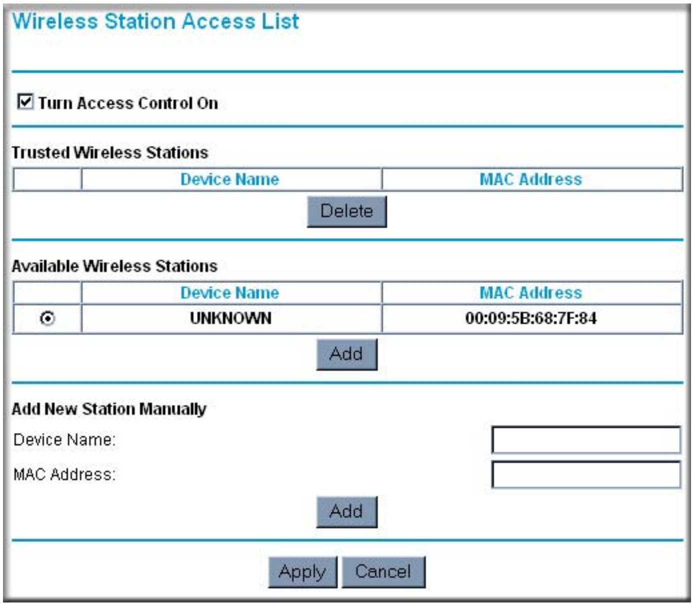
⚠	**Warning:** The SSID of any wireless access adapters must match the SSID you configure in the DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router. If they do not match, you will not get a wireless connection.

Restricting Wireless Access Based on the Wireless Station Access List

This list determines which wireless hardware devices will be allowed to connect to the wireless modem router.

To restrict access based on MAC addresses, follow these steps:

1. Log in to the wireless 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. From the Wireless Settings menu, Wireless Station Access List section, click the **Setup Access List** button to display the list, shown below:



Wireless Station Access List

☑ Turn Access Control On

Trusted Wireless Stations

	Device Name	MAC Address

Available Wireless Stations

	Device Name	MAC Address
●	UNKNOWN	00:09:5B:68:7F:84

Add New Station Manually

Device Name:

MAC Address:

Figure 3-3

3. Select the **Turn Access Control On** check box to enable the restricting of wireless computers by their MAC addresses.
4. If the wireless station is currently connected to the network, you can select it from the Available Wireless Stations list. Click **Add** to add the station to the Trusted Wireless Stations list.

5. If the wireless station is not currently connected, you can enter its address manually. Enter the MAC address of the authorized computer. The MAC address is usually printed on the wireless card, or it may appear in the wireless modem router's DHCP table. The MAC address will be 12 hexadecimal digits.

   Click **Add** to add your entry. You can add several stations to the list, but the entries will be discarded if you do not click Apply.

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

   > **Note:** If you are configuring the wireless modem router from a wireless computer whose MAC address is not in the Trusted Wireless Stations list, and you select Trusted Wireless Stations only, you will lose your wireless connection when you click **Apply**. You must then access the wireless modem router from a wired computer to make any further changes.

6. Make sure the **Turn Access Control On** check box is selected, then click **Apply**.

Now, only devices on this list will be allowed to wirelessly connect to the wireless modem router. This prevents unauthorized access to your network.

How to Configure WPA-PSK/WPA2-PSK Security

A high performance client like the NETGEAR WN511B must connect using WPA2-PSK in order to achieve maximum performance. Wireless clients that connect to this router using WPA-PSK will run at no more than 802.11g speed. This option allows wireless clients to use either encryption method.

> **Note:** Not all wireless adapters support WPA or WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK + WPA2-PSK, follow these steps:

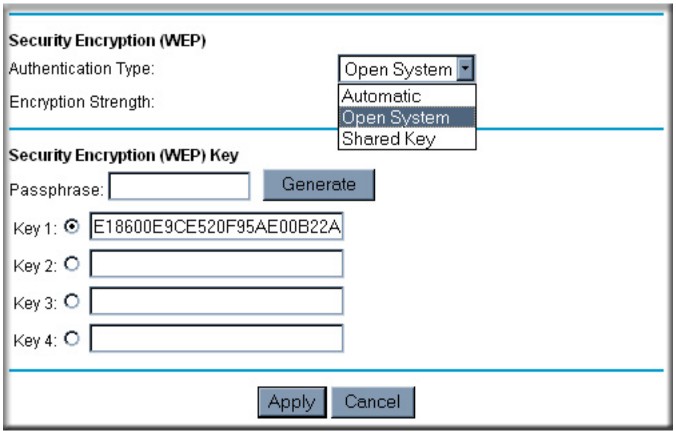
1. Log in at the default LAN address of *http://192.168.0.1,* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the Setup section of the main menu of the DG834N.
3. Choose the **WPA-PSK [TKIP] + WPA2-PSK [AES]** radio button. The WPA-PSK menu will open.
4. Enter the pre-shared key in the Passphrase field using between 8 and 63 characters.
5. Click **Apply** to save your settings.

If the wireless network mode is set to “g and b”, you have the option of selecting WPA-PSK only, WPA2-PSK only, WPA-802.1x, and WPA2-802.1x. For details about the 802.1x authentication options, refer to “How to Configure WPE-802.1x or WPE2-802.1x” on page 3-14.

Choosing Alternative Authentication and Encryption Methods

Note: Alternative authentication and encryption methods are only available if you select “g and b” as the wireless network mode in the Wireless Settings menu. These options will result in a performance impact since wireless communications will be limited to the 802.11g data rate.

Understanding WEP Authentication and Security Encryption



Security Encryption (WEP)

Authentication Type: Open System

Encryption Strength:

Security Encryption (WEP) Key

Passphrase:

Key 1: ● E18600E9CE520F95AE00B22A

Key 2: ○

Key 3: ○

Key 4: ○

Figure 3-4

Restricting wireless access prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the WEP data encryption settings described below will prevent a determined intruder from eavesdropping on your wireless data communications. Also, if you are using the Internet for such activities as purchases or banking, those Internet sites use another level of highly secure encryption called SSL. You can tell if a web site is using SSL because the web address begins with HTTPS rather than HTTP.

Authentication Type Selection . The DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router lets you select the following WEP wireless authentication schemes.

- Automatic
- Open System

Please refer to "Preparing a Computer for Network Access:" in Appendix B for a full explanation of each of these options, as defined by the IEEE 802.11g wireless communication standard.

Encryption Choices. Please refer to "Preparing a Computer for Network Access:" in Appendix B for a full explanation of each of the following choices, as defined by the IEEE 802.11g wireless communication standard. Choose the encryption strength from the drop-down list:

64 or 128 bit WEP. When 64 Bit WEP or 128 Bit WEP is selected, WEP encryption will be applied.

If WEP is enabled, 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.

There are two methods for creating WEP encryption keys:

- Passphrase. Enter a word or group of printable characters in the Passphrase box and click the Generate button.
- Manual. 64-bit WEP: Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: Enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

Select the radio button for the key you want to make active.

How to Configure WEP

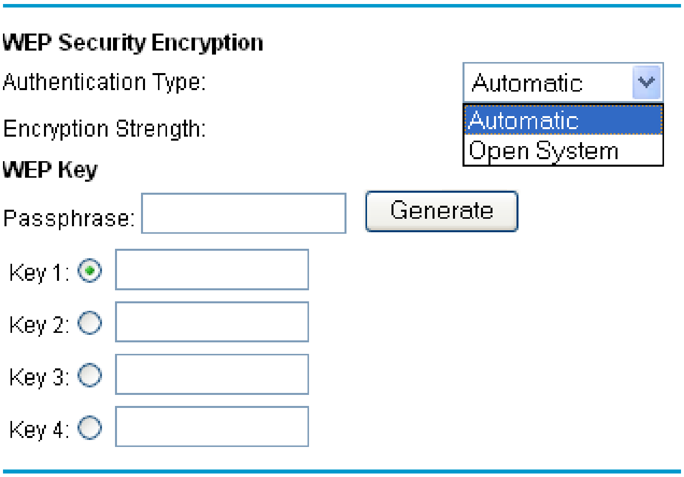
To configure WEP data encryption, follow these steps:

1. Log in to the wireless 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. Click the Wireless Settings link in the main menu of the wireless modem router.

3. In the Security Options portion of the page, select WEP.

> **Note:** The WEP security option is only available if the wireless network mode is set to “g and b”.

4. Go to the WEP Security Encryption portion of the page:



WEP Security Encryption

Authentication Type: Automatic

Encryption Strength:

WEP Key

Passphrase:

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Figure 3-5

5. Select the Authentication Type.

6. Select the Encryption Strength setting.

7. 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.

- Automatic — enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
- Manual — enter hexadecimal digits (any combination of 0-9, a-f, or A-F).
  Select which of the four keys will be active.

8. Select the radio button for the key you want to make active.

Be sure you clearly understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one included in Windows XP only allow entry of one key which must match the default key you set in the DG834N.

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

> **Note:** When configuring the wireless modem router from a wireless computer, if you configure WEP settings, you will lose your wireless connection when you click Apply. You must then either configure your wireless adapter to match the wireless modem router WEP settings or access the wireless modem router from a wired computer to make any further changes.

How to Configure WPE-802.1x or WPE2-802.1x

This version of WPA requires the use of a Radius server for authentication. Each user (Wireless Client) must have a "user" login on the Radius Server, and the wireless modem router must have a "client" login on the Radius server. Data transmissions are encrypted using a key that is automatically generated.

1. Log in to the wireless 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. Click the Wireless Settings link in the main menu of the wireless modem router.
3. In the Security Options portion of the page, select WPE-802.1x or WPE2-802.1x.

> **Note:** The WPE-802.1x and WPE2-802.1x security options are only available if the wireless network mode is set to “g and b”.

4. In the **Radius Server Name/IP Address** text box, enter the name or IP address of the Radius Server on your LAN. This is a required field.
5. In the **Radius Port** field, enter the port number used for connections to the Radius server.
6. In the **Radius Shared Key** field, enter the desired value for the Radius shared key. This key enables the **wireless modem router** to log in to the Radius server and must match the “client” login value used on the Radius server.

Chapter 4
Protecting Your Network

This chapter describes how to use the basic firewall features of the DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router to protect your network.

Protecting Access to Your Wireless Modem Router

For security reasons, the wireless modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter **admin** for the wireless modem router user name and **password** for the wireless modem router password. You can use procedures below to change the wireless modem router's password and the amount of time for the administrator's login timeout.

➡	**Note:** The user name and password are not the same as any user name or password your may 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.

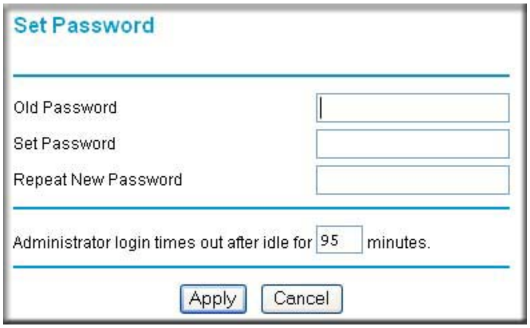
How to Change the Built-In Password

1. Log in to the wireless 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 wireless modem router.

http://192.168.0.1

Figure 4-1

2. From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in Figure 4-2.



Set Password

Old Password

Set Password

Repeat New Password

Administrator login times out after idle for 95 minutes.

Figure 4-2

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 will be required to log in again to continue the configuration. If you have backed up the wireless modem router settings previously, you should do a new backup so that the saved settings file includes the new password.

Changing the Administrator Login Timeout

For security, the administrator's login to the wireless modem router configuration will timeout after a period of inactivity. To change the login timeout period:

1. In the Set Password menu, type a number in ‘Administrator login times out’ field. The suggested default value is 5 minutes.
2. Click Apply to save your changes or click Cancel to keep the current period.

Configuring Basic Firewall Services

Basic firewall services you can configure include access blocking and scheduling of firewall security. These topics are presented below.

Blocking Keywords, Sites, and Services

The wireless modem router provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the RangeMax NEXT Wireless ADSL2+ Modem Router prevents objectionable content from reaching your PCs. The wireless modem router allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

- Keyword blocking of HTTP traffic.
- Outbound Service Blocking limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of Service (DoS) protection. Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

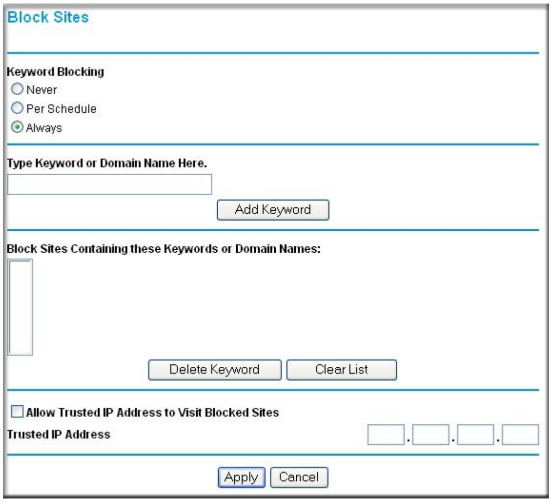
The section below explains how to configure your wireless modem router to perform these functions.

How to Block Keywords and Sites

The RangeMax NEXT Wireless ADSL2+ Modem Router allows you to restrict access to Internet content based on functions such as Web addresses and Web address keywords.

1. Log in to the wireless 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 may have previously set for the wireless modem router.

2. Select the Block Sites link of the Security menu.



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 4-3

3. To enable keyword blocking, select one of the following:
   - Per Schedule—to turn on keyword blocking according to the settings on the Schedule page.
   - Always—to turn on keyword blocking all of the time, independent of the Schedule page.
4. Enter a keyword or domain in the Keyword box, click Add Keyword, then click Apply.

   Some examples of Keyword application follow:
   - If the keyword “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
   - If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
   - Enter the keyword “.” to block all Internet browsing access.

   Up to 32 entries are supported in the Keyword list.
5. To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.
6. To specify a trusted user, enter that computer’s IP address in the Trusted IP Address box and click Apply.

You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.

7. Click Apply to save your settings.

Firewall Rules

Firewall rules are used to block or allow specific traffic passing through from one side of the router to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

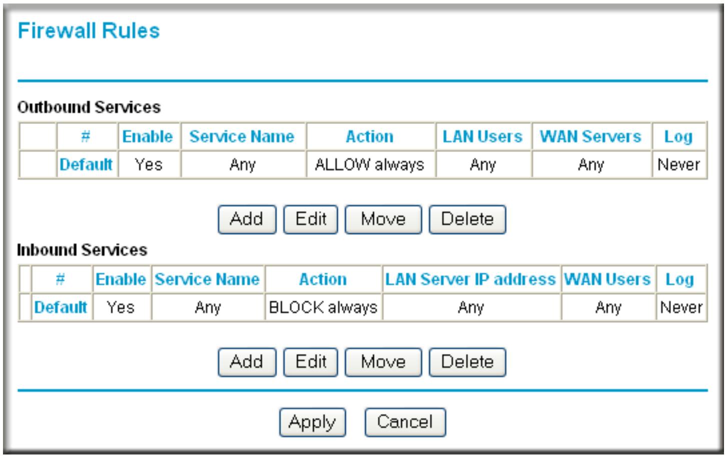
A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the DG834N are:

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

You can define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

You can change the order of precedence of rules so that the rule that applies most often will take effect first. See “Order of Precedence for Rules” on page 4-11 for more details.

To access the rules configuration of the DG834N, click the Firewall Rules link on the main menu, then click Add for either an Outbound or Inbound Service.



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

Figure 4-4

- To edit an existing rule, select its button on the left side of the table and click Edit.
- To delete an existing rule, select its button on the left side of the table and click Delete.
- To move an existing rule to a different position in the table, select its button on the left side of the table and click Move. At the script prompt, enter the number of the desired new position and click OK.

Inbound Rules (Port Forwarding)

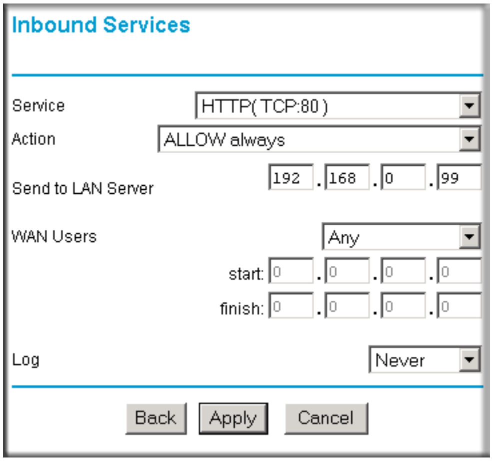
Because the wireless modem router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the wireless modem router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day. This rule is shown in Figure 4-5:



Inbound Services

Service: HTTP(TCP:80)
Action: ALLOW always
Send to LAN Server: 192 . 168 . 0 . 99
WAN Users: Any
start: 0 . 0 . 0 . 0
finish: 0 . 0 . 0 . 0
Log: Never

Figure 4-5

The parameters are:

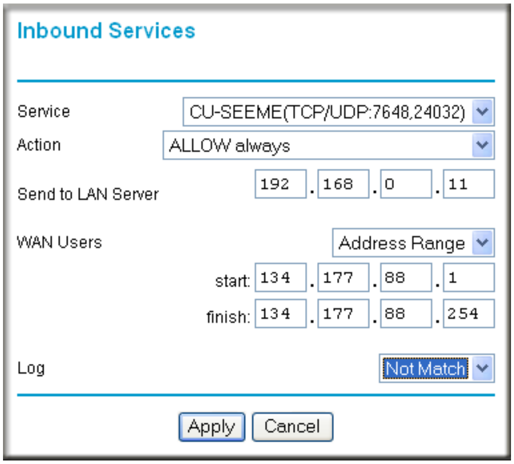
- **Service**: From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services menu, see "How to Define Services" on page 4-12, to add any additional services or applications that do not already appear.
- **Action**: Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **Send to LAN Server**: Enter the IP address of the computer or server on your LAN which will receive the inbound traffic covered by this rule.
- **WAN Users**: These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:
  - **Any**: All 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 field.

- **Log**: You can select whether the traffic will be logged. The choices are:
  - **Never:** No log entries will be made for this service.
  - **Always**: Any traffic for this service type will be logged.
  - **Match**: Traffic of this type that matches the parameters and action will be logged.
  - **Not match**: Traffic of this type that does not match the parameters and action will be logged.

Inbound Rule Example: Allowing Video conferencing

If you want to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in Figure 4-6, CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.



Inbound Services

Service: CU-SEEME(TCP/UDP:7648,24032)

Action: ALLOW always

Send to LAN Server: 192 . 168 . 0 . 11

WAN Users: Address Range

start: 134 . 177 . 88 . 1

finish: 134 . 177 . 88 . 254

Log: Not Match

Figure 4-6

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menu so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer's IP address constant.

- Local computers must access the local server using the computer’s local LAN address (192.168.0.11 in the example in Figure 4-6 above). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

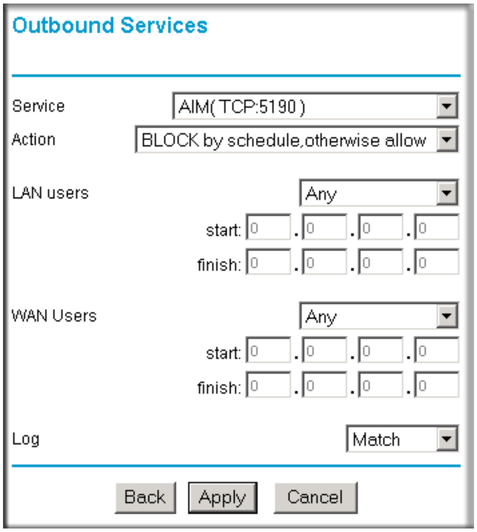
The wireless modem router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on

- IP address of the local computer (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Following is an application example of outbound rules:

Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the wireless modem router log any attempt to use Instant Messenger during that blocked period.



Outbound Services

Service: AIM(TCP:5190)

Action: BLOCK by schedule,otherwise allow

LAN users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

WAN Users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Match

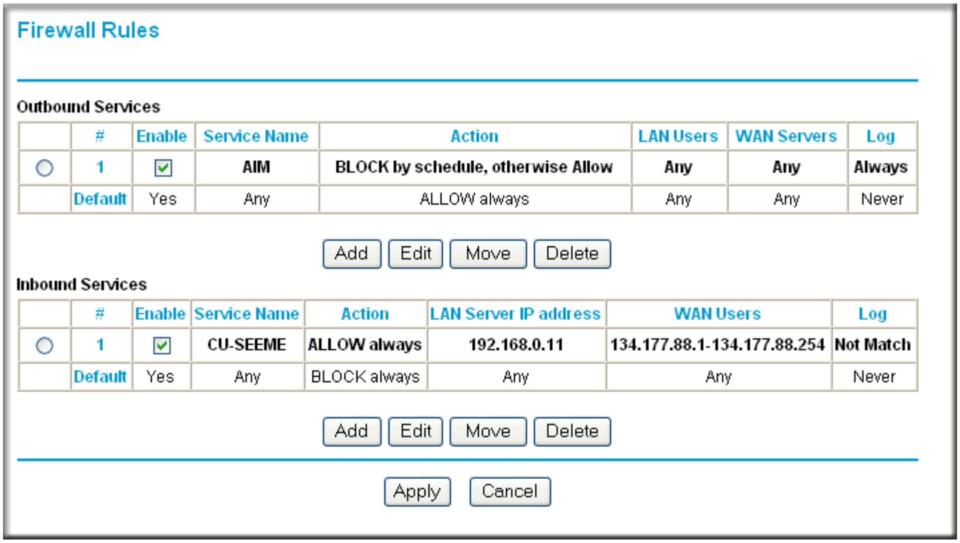
Figure 4-7

The parameters are:

- **Service**: From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Add Custom Service feature to add any additional services or applications that do not already appear.
- **Action**: Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **LAN Users**: These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:
  - **Any**: All 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 field.
- **WAN Users**:These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the desired option:
  - **Any**: All 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 field.
- **Log:** You can select whether the traffic will be logged. The choices are:
  - **Never**: No log entries will be made for this service.
  - **Always**: Any traffic for this service type will be logged.
  - **Match**: Traffic of this type that matches the parameters and action will be logged.
  - **Not match**: Traffic of this type that does not match the parameters and action will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in Figure 4-8:



Firewall Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
○	1	☑	AIM	BLOCK by schedule, otherwise Allow	Any	Any	Always
	Default	Yes	Any	ALLOW always	Any	Any	Never

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
○	1	☑	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1-134.177.88.254	Not Match
	Default	Yes	Any	BLOCK always	Any	Any	Never

Figure 4-8

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

Services

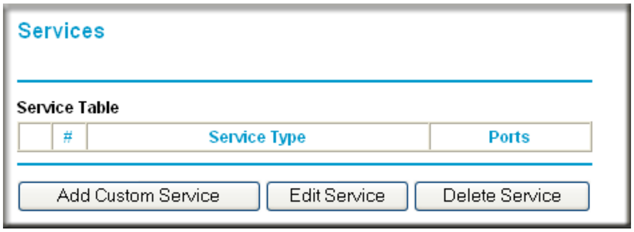
Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server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

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the wireless modem router already holds a list of many service port numbers, you are not limited to these choices. Use the procedure below to create your own service definitions.

How to Define Services

1. Log in to the wireless 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 wireless modem router.
2. Select the Services link of the Security menu to display the Services menu shown in Figure 4-9:



Services

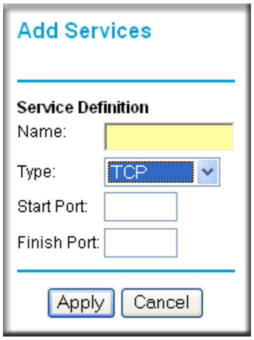
Service Table

	#	Service Type	Ports

Figure 4-9

- To create a new Service, click the **Add Custom Service** button.
- To edit an existing Service, select its button on the left side of the table and click **Edit Service**.
- To delete an existing Service, select its button on the left side of the table and click **Delete Service**.

3. Use the page shown below to define or edit a service.



Add Services

Service Definition

Name:

Type: TCP

Start Port:

Finish Port:

Figure 4-10

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

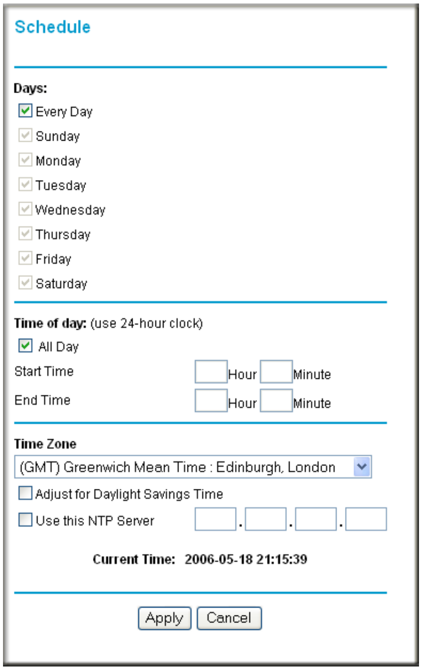
Setting Times and Scheduling Firewall Services

The RangeMax NEXT Wireless ADSL2+ 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.

How to Set Your Time Zone

In order to localize the time for your log entries, you must specify your Time Zone:

1. Log in to the wireless 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 wireless modem router.
2. Select the Schedule link of the Security menu to display the menu shown below.



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: 2006-05-18 21:15:39

Figure 4-11

3. Select your Time Zone. This setting will be used for the blocking schedule according to your local time zone and for time-stamping log entries.

Select the Adjust for daylight savings time check box if your time zone is currently in daylight savings time.

Note: If your region uses Daylight Savings Time, you must manually select Adjust for Daylight Savings Time on the first day of Daylight Savings Time, and clear it at the end. Enabling Daylight Savings Time will cause one hour to be added to the standard time.

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

How to Schedule Firewall Services

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

1. Log in to the wireless 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 wireless modem router.
2. Select the Schedule link of the Security menu to display menu shown above in Figure 4-11.
3. To block Internet services based on a schedule, select Every Day or select one or more days. If you want to limit access completely for the selected days, select All Day. Otherwise, to limit access during certain times for the selected days, enter Start Blocking and End Blocking times.

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

4. Click Apply to save your changes.

Chapter 5
Managing Your Network

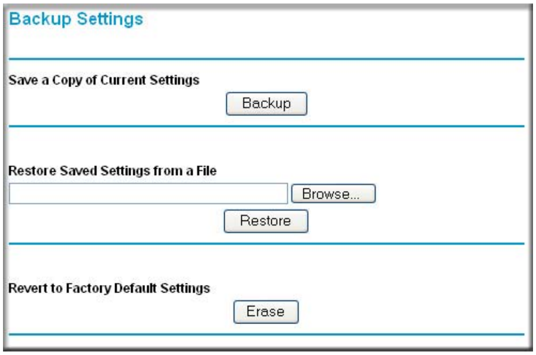
This chapter describes how to perform network management tasks with your DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the RangeMax NEXT Wireless ADSL2+ Modem Router are stored in a configuration file in the wireless modem router. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.

How to Back Up the Configuration to a File

1. Log in to the wireless 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 User Name, Password and LAN address you have chosen for the wireless modem router.
2. From the Maintenance heading of the Main Menu, select the Backup Settings menu as seen in Figure 5-1.



Backup Settings

Save a Copy of Current Settings

Restore Saved Settings from a File

Revert to Factory Default Settings

Figure 5-1

3. Click Backup to save a copy of the current settings.

4. Store the `.cfg` file on a computer on your network.

How to Restore the Configuration from a File

1. Log in to the wireless 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 User Name, Password and LAN address you have chosen for the wireless modem router.
2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in Figure 5-1.
3. Enter the full path to the file on your network or click the Browse button to locate the file.
4. When you have located the `.cfg` file, click the Restore button to upload the file to the wireless modem router.
5. The wireless modem router will then reboot automatically.

How to Erase the Configuration

It is sometimes desirable to restore the wireless modem router to the factory default settings. This can be done by using the Erase function.

1. To erase the configuration, from the Maintenance menu Settings Backup link, click the Erase button on the screen.
2. The wireless modem router will then reboot automatically.

   After an erase, the wireless modem router's password will be **password**, the LAN IP address will be 192.168.0.1, and the wireless modem router's DHCP client will be enabled.

Note: To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the wireless modem router. See Figure 1-2.

Upgrading the Wireless Modem Router’s Firmware

The software of the RangeMax NEXT Wireless ADSL2+ Modem Router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

Upgrade files can be downloaded from NETGEAR's Web site. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN or .IMG) file before uploading it to the wireless modem router.

How to Upgrade the Wireless Modem Router Firmware

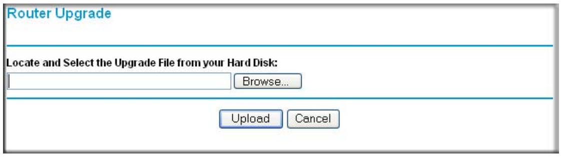
Note: NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you may need to restore your configuration settings.

1. Download and unzip the new software file from NETGEAR.

   The Web browser used to upload new firmware into the wireless modem router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or above.

2. Log in to the wireless 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 User Name, Password and LAN address you have chosen for the wireless modem router.

3. From the Main Menu of the browser interface, under the Maintenance heading, select the **Router Upgrade** heading to display the menu shown in Figure 5-2.



Router Upgrade

Locate and Select the Upgrade File from your Hard Disk:

Figure 5-2

4. In the Wireless Modem Router Upgrade menu, click the **Browse** to locate the binary (.BIN or .IMG) upgrade file.

5. Click **Upload**.

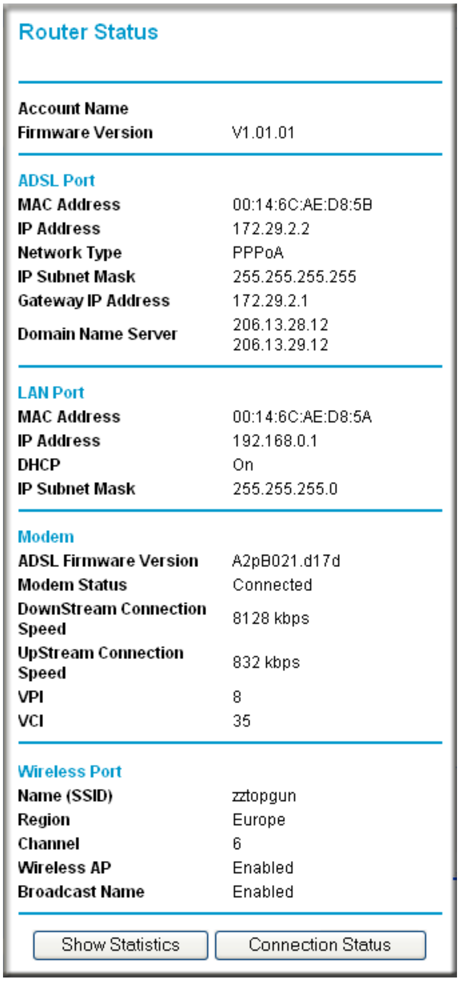
➡	**Note:** When uploading software to the wireless modem router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your wireless modem router will automatically restart. The upgrade process will typically take about one minute. In some cases, you may need to clear the configuration and reconfigure the wireless modem router after upgrading.

Network Management Information

The DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router provides a variety of status and usage information which is discussed below.

Viewing Wireless Modem Router Status and Usage Statistics

From the Main Menu, under Maintenance, select Wireless Modem Router Status to view the screen in Figure 5-3.



Router Status

Account Name	
Firmware Version	V1.01.01
ADSL Port	
MAC Address	00:14:6C:AE:D8:5B
IP Address	172.29.2.2
Network Type	PPPoA
IP Subnet Mask	255.255.255.255
Gateway IP Address	172.29.2.1
Domain Name Server	206.13.28.12 206.13.29.12
LAN Port	
MAC Address	00:14:6C:AE:D8:5A
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
Modem	
ADSL Firmware Version	A2pB021.d17d
Modem Status	Connected
DownStream Connection Speed	8128 kbps
UpStream Connection Speed	832 kbps
VPI	8
VCI	35
Wireless Port	
Name (SSID)	zztopgun
Region	Europe
Channel	6
Wireless AP	Enabled
Broadcast Name	Enabled

Figure 5-3

The Wireless Modem Router Status menu provides status and usage information.

This screen shows the following parameters:

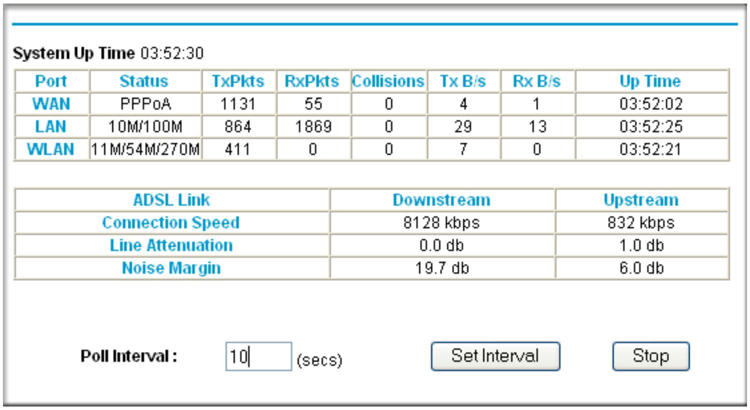
Table 5-1. Menu 3.2 - Wireless Modem Router Status Fields

Field	Description
Account Name	The Host Name assigned to the wireless modem router in the Basic Settings menu.
Firmware Version	This field displays the wireless modem router firmware version.
ADSL Port	These parameters apply to the Internet (ADSL) port of the wireless modem router.
MAC Address	This field displays the Ethernet MAC address being used by the Internet (ADSL) port of the wireless modem router.
IP Address	This field displays the IP address being used by the Internet (ADSL) port of the wireless modem router. If no address is shown, the wireless modem router cannot connect to the Internet.
Network Type	The network type will depend upon your ISP.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (ADSL) port of the wireless modem router.
Gateway IP Address	IP address used as a gateway to the internet for computers configured to use DHCP
Domain Name Server (DNS)	This field displays the DNS Server IP addresses being used by the wireless modem router. These addresses are usually obtained dynamically from the ISP.
LAN Port	These parameters apply to the Local (ADSL) port of the wireless modem router.
MAC Address	This field displays the Ethernet MAC address being used by the Local (LAN) port of the wireless modem router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the wireless modem router. The default is 192.168.0.1.
DHCP	If OFF, the wireless modem router will not assign IP addresses to PCs on the LAN. If ON, the wireless modem router will assign IP addresses to PCs on the LAN.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the wireless modem router. The default is 255.255.255.0.
Modem	These parameters apply to the Local (WAN) port of the wireless modem router.
ADSL Firmware Version	The version of the firmware.

Table 5-1. Menu 3.2 - Wireless Modem Router Status Fields (continued)

Field	Description
Modem Status	The connection status of the modem.
Downstream Connection Speed	The speed at which the modem is receiving data from the ADSL line.
Upstream Connection Speed	The speed at which the modem is transmitting data to the ADSL line.
VPI	The Virtual Path Identifier setting.
VCI	The Virtual Channel Identifier setting.
Wireless Port	These are the settings as set in the Wireless Settings page; see "Understanding Wireless Settings" in Chapter 3 for details.
Name (SSID)	The Service Set ID, also known as the wireless network name.
Region	The country where the unit is set up for use.
Channel	The current channel, which determines the operating frequency.
Wireless AP	Indicates if the Access Point feature is disabled or not. If not enabled, the Wireless LED on the front panel will be off.
Broadcast Name	Indicates if the DG834N is configured to broadcast its SSID.

Click the **Show Statistics** button to display wireless modem router usage statistics, as shown in Figure 5-3 below:



System Up Time 03:52:30

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoA	1131	55	0	4	1	03:52:02
LAN	10M/100M	864	1869	0	29	13	03:52:25
WLAN	11M/54M/270M	411	0	0	7	0	03:52:21

ADSL Link	Downstream	Upstream
Connection Speed	8128 kbps	832 kbps
Line Attenuation	0.0 db	1.0 db
Noise Margin	19.7 db	6.0 db

Poll Interval : 10 (secs)

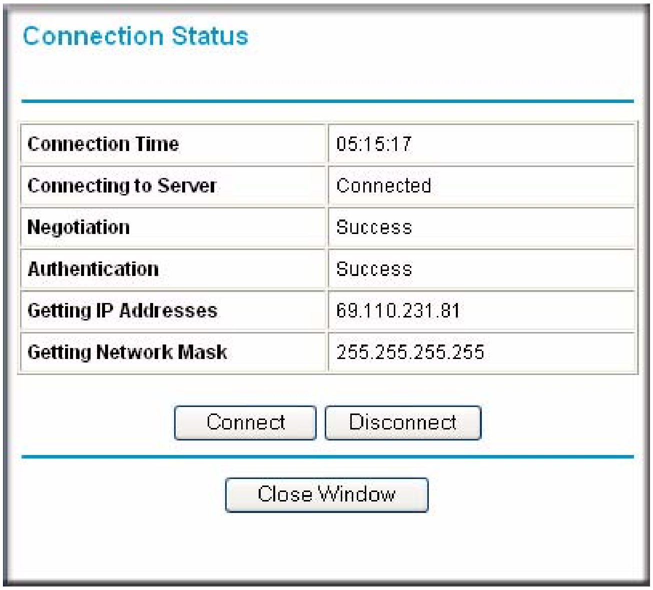
Figure 5-4

This screen shows the following statistics:.

Table 5-2. Router Statistics Fields

Field	Description
WAN, LAN, or WLAN	The statistics for the WAN (Internet), LAN (local), and Wireless LAN (WLAN) ports. For each port, the screen displays:
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 line utilization—percentage of current bandwidth used on this port.
Rx B/s	The average line utilization for this port.
Up Time	The time elapsed since the last power cycle or reset.
ADSL Link Downstream or Upstream	The statistics for the upstream and downstream ADSL link. These statistics will be of interest to your technical support representative if you are having problems obtaining or maintaining a connection.
Connection Speed	Typically, the downstream speed is faster than the upstream speed.
Line Attenuation	The line attenuation will increase the further you are physically located from your ISP's facilities.
Noise Margin	This is the signal-to-noise ratio and is a measure of the quality of the signal on the line.
Poll Interval	Specifies the interval at which the statistics are updated in this window. Click Stop to freeze the display.

Click the Connection Status button to display wireless modem router connection status, as shown in Figure 5-5 below:



Connection Status

Connection Time	05:15:17
Connecting to Server	Connected
Negotiation	Success
Authentication	Success
Getting IP Addresses	69.110.231.81
Getting Network Mask	255.255.255.255

Figure 5-5

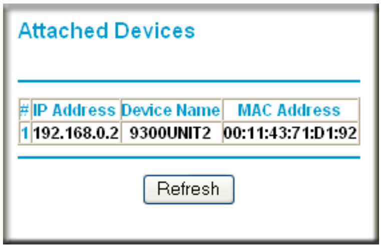
This screen shows the following statistics:

Table 5-3. Connection Status Fields (PPPoE Network Type Example)

Field	Description
Connection Time	The time elapsed since the last connection to the Internet via the ADSL port.
Connecting to Sender	The connection status.
Negotiation	Success or Failed
Authentication	Success or Failed
IP Address	The IP Address assigned to the WAN port by the ADSL Internet Service Provider.
Network Mask	The Network Mask assigned to the WAN port by the ADSL Internet Service Provider.

Viewing Attached Devices

The Attached Devices menu contains a table of all IP devices that the wireless modem router has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown in Figure 5-6:



Attached Devices

#	IP Address	Device Name	MAC Address
1	192.168.0.2	9300UNIT2	00:11:43:71:D1:92

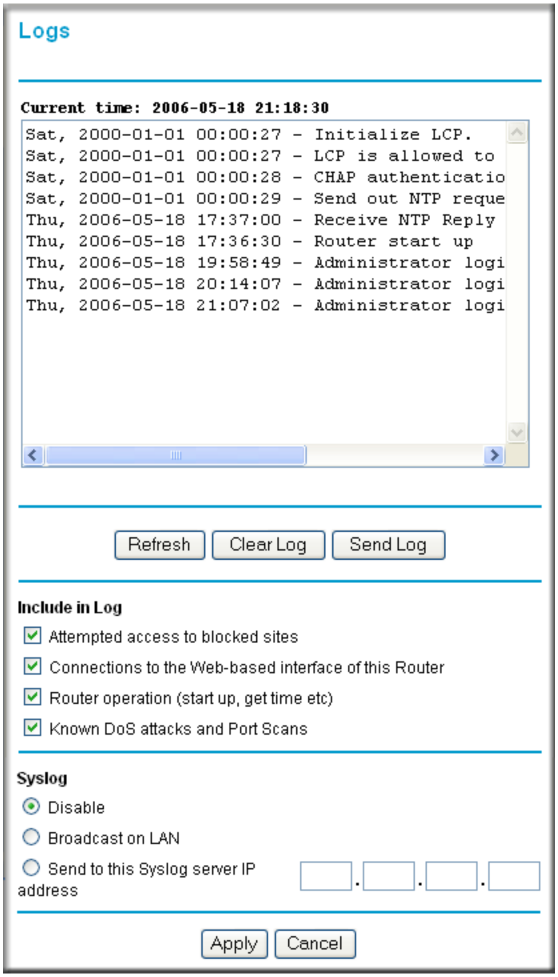
Figure 5-6

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

Viewing, Selecting, and Saving Logged Information

The wireless modem router will log security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites menu, the Logs page can show you when someone on your network tries to access a blocked site. If you enabled e-mail notification, you will receive these logs in an e-mail message. If you do not have e-mail notification enabled, you can view the logs here.

An example of the logs file is shown below.



Logs

Current time: 2006-05-18 21:18:30

```
Sat, 2000-01-01 00:00:27 - Initialize LCP.
Sat, 2000-01-01 00:00:27 - LCP is allowed to
Sat, 2000-01-01 00:00:28 - CHAP authenticatio
Sat, 2000-01-01 00:00:29 - Send out NTP reque
Thu, 2006-05-18 17:37:00 - Receive NTP Reply
Thu, 2006-05-18 17:36:30 - Router start up
Thu, 2006-05-18 19:58:49 - Administrator logi
Thu, 2006-05-18 20:14:07 - Administrator logi
Thu, 2006-05-18 21:07:02 - 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 5-7

Log entries are described in Table 5-4 below:

Table 5-4. Security Log entry descriptions

Field	**Description**
Date and Time	The date and time the log entry was recorded.
Description or Action	The type of event and what action was taken if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN
Destination	The name or IP address of the destination device or Web site.
Destination port and interface	The service port number of the destination device, and whether it's on the LAN or WAN.

Log action buttons are described in Table 5-5 below:

Table 5-5. Security Log action buttons

Field	**Description**
Refresh	Refresh the log screen.
Clear Log	Clear the log entries.
Send Log	Email the log immediately.
Apply	Apply the current settings.
Cancel	Clear the current settings.

Selecting What Information to Log

Besides the standard information listed above, you can choose to log additional information. Those optional selections are as follows:

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

Saving Log Files on a Server

You can choose to write the logs to a computer running a syslog program. To activate this feature, select to **Broadcast on Lan** or enter the IP address of the server where the Syslog file will be written.

Examples of Log Messages

Following are examples of log messages. In all cases, the log entry shows the timestamp as: Day, Year-Month-Date Hour:Minute:Second

Activation and Administration

```
Tue, 2006-05-21 18:48:39 - NETGEAR activated
```

[This entry indicates a power-up or reboot with initial time entry.]

```
Tue, 2006-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2
Thu, 2006-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

[This entry shows an administrator logging in and out from IP address 192.168.0.2.]

```
Tue, 2006-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

[This entry shows a time-out of the administrator login.]

```
Wed, 2006-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was emailed.]

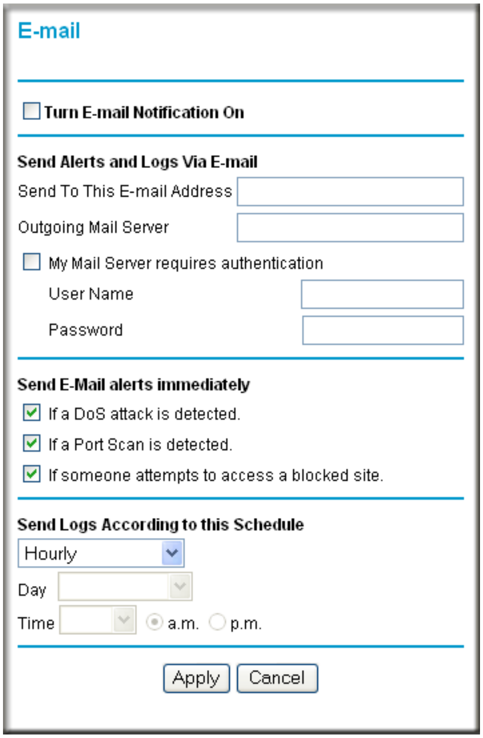
Dropped Packets

```
Wed, 2006-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
Sun, 2006-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
Sun, 2006-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

[These entries show an inbound FTP (port 21) packet, User Datagram Protocol (UDP) packet (port 6970), and Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

Enabling Security Event E-mail Notification

In order to receive logs and alerts by e-mail, you must provide your e-mail information in the E-mail subheading:



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.

Apply Cancel

Figure 5-8

- **Turn e-mail notification on**. Select this check box if you want to receive e-mail logs and alerts from the wireless modem router.
- **Send To This E-mail Address**—Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.
- **Outgoing Mail Server**. Enter the name or IP address of your ISP’s outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.

- **My Mail Server requires authentication**—If you use an outgoing mail server provided by your current ISP, you do not need to check this box. If you use an e-mail account that is not provided by your ISP, check this box and enter the required user name and password information.
- **Send E-Mail alerts immediately.** Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule.** Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - Day for sending log
    Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
  - Time for sending log
    Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

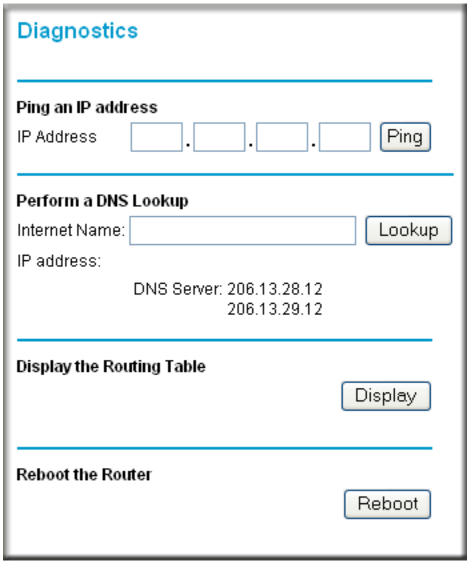
  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the wireless modem router's memory. If the wireless modem router cannot e-mail the log file,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

Running Diagnostic Utilities and Rebooting the Wireless Modem Router

The RangeMax NEXT Wireless ADSL2+ Modem Router has a diagnostics feature. You can use the diagnostics menu to perform the following functions from the wireless 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 wireless modem routers the wireless modem router is communicating with.
- Reboot the wireless modem router to enable new network configurations to take effect or to clear problems with the wireless modem router's network connection.

From the Main Menu of the browser interface, under the Maintenance heading, select the Wireless Modem Router Diagnostics heading to display the menu shown in Figure 5-9.


Diagnostics

Ping an IP address

IP Address . . .

Perform a DNS Lookup

Internet Name:

IP address:

DNS Server: 206.13.28.12
206.13.29.12

Display the Routing Table

Reboot the Router

Figure 5-9

Enabling Remote Management

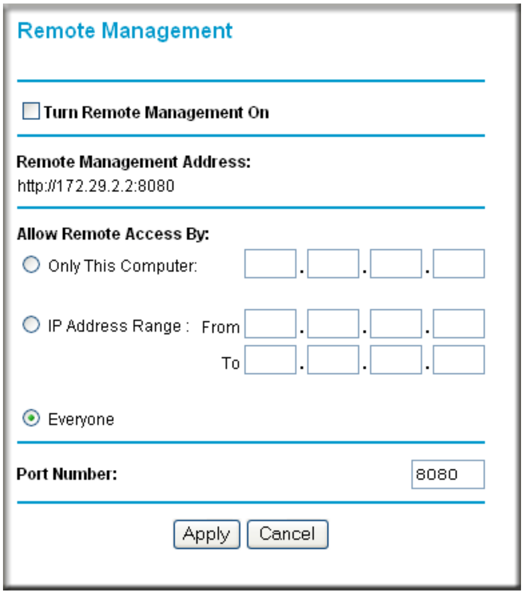
Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router.

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

Configuring Remote Management

1. Log in to the wireless 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 User Name, Password and LAN address you have chosen for the wireless modem router.

2. From the Advanced section of the main menu, select the Remote Management link.



Remote Management

□ Turn Remote Management On

Remote Management Address:
http://172.29.2.2:8080

Allow Remote Access By:

○ Only This Computer: ___ . ___ . ___ . ___

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

● Everyone

Port Number: 8080

Figure 5-10

3. Select the **Turn Remote Management On** check box.

4. Specify what external addresses will be allowed to access the wireless modem router’s remote management. For 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.

5. Specify the Port Number that will be used for accessing the management interface.

   Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

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

When accessing your wireless modem router from the Internet, you will type your wireless modem router's WAN IP address in your browser's Address box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter in your browser:

```
http://134.177.0.123:8080
```

➡	**Note:** In this case, the http:// must be included in the address.

Chapter 6
Advanced Configuration

This chapter describes how to configure the advanced features of your DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router.

Configuring Advanced Security

The DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router provides a variety of advanced features, such as:

- Setting up a Demilitarized Zone (DMZ) Server
- Connecting Automatically, as Required
- Disabling Port Scan and DOS Protection
- Responding to a Ping on the Internet WAN Port
- MTU Size
- Flexibility on configuring your LAN TCP/IP settings
- Using the Router as a DHCP Server
- Configuring Dynamic DNS
- Configuring Static Routes

These features are discussed below.

Setting Up A Default DMZ Server

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

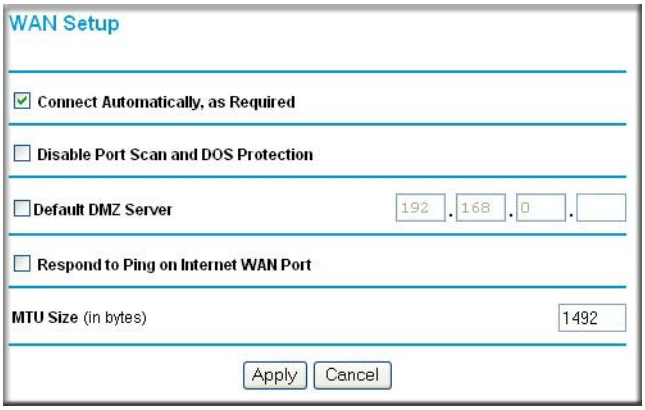
Note: For security reasons, you should avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

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

How to Configure a Default DMZ Server

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

1. Log in to the wireless 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 wireless modem router.
2. From the Main Menu, under Advanced, click the WAN Setup link to view the page shown in Figure 6-1:



WAN Setup

☑ Connect Automatically, as Required

□ Disable Port Scan and DOS Protection

□ Default DMZ Server 192 . 168 . 0 .

□ Respond to Ping on Internet WAN Port

MTU Size (in bytes) 1492

Figure 6-1

3. Select the **Default DMZ Server** check box.
4. Type the IP address for that server.
5. Click **Apply** to save your changes.

Connect Automatically, as Required

Normally, this option should be enabled, so that an Internet connection will be made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting.

If disabled, you must connect manually, using the sub-screen accessed from the "Connection Status" button on the Status screen.

If you have an "Always on" connection, this setting has no effect.

Disable Port Scan and DOS Protection

The Firewall protects your LAN against Port Scans and Denial of Service (DOS) attacks. This should be disabled only in special circumstances.

Respond to Ping on Internet WAN Port

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

MTU Size

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

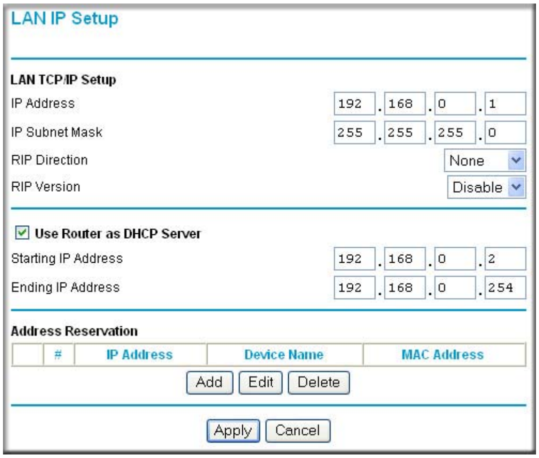
Configuring LAN IP Settings

The LAN IP Setup menu allows configuration of LAN IP services such as DHCP and RIP. These features can be found under the Advanced heading in the Main Menu of the browser interface.

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

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

These addresses are part of the Internet Engineering Task Force (IETF)-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.



LAN IP Setup

LAN TCP/IP Setup

IP Address	192 . 168 . 0 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	None
RIP Version	Disable

☑ 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 6-2

The LAN TCP/IP Setup parameters are:

- **IP Address:** This is the LAN IP address of the wireless modem router.
- **IP Subnet Mask:** This is the LAN Subnet Mask of the wireless modem router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or wireless modem router.
- **RIP Direction:** RIP (Router Information Protocol) allows a wireless modem router to exchange routing information with other routers. The RIP Direction selection controls how the Wireless Modem Router sends and receives RIP packets. Both is the default.
  - When set to **Both** or **Out Only**, the wireless modem router will broadcast its routing table periodically.
  - When set to **Both** or **In Only**, it will incorporate the RIP information that it receives.
  - When set to **None**, it 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 wireless modem router sends. It recognizes both formats when receiving. By default, this is set for RIP-1.
  - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.

- RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
  - RIP-2B uses subnet broadcasting.
  - RIP-2M uses multicasting.

➡ **Note:** If you change the LAN IP address of the wireless 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.

DHCP

By default, the wireless modem router will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the wireless modem router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

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

Use Router as DHCP server

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the 'Use router as DHCP server' check box. Otherwise, leave it selected.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you may want to save part of the range for devices with fixed addresses.

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

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address is the router's LAN IP address
- Primary DNS Server, if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router's LAN IP address

- Secondary DNS Server, if you entered a Secondary DNS address in the Basic Settings menu
- WINS Server, short for *Windows Internet Naming Service Server,* determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

Reserved IP addresses

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

To reserve an IP address:

1. Click the **Add** button.

2. In the IP Address box, type the IP address to assign to the computer or server.
Choose an IP address from the router's LAN subnet, such as 192.168.0.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 menu and paste it here.

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

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

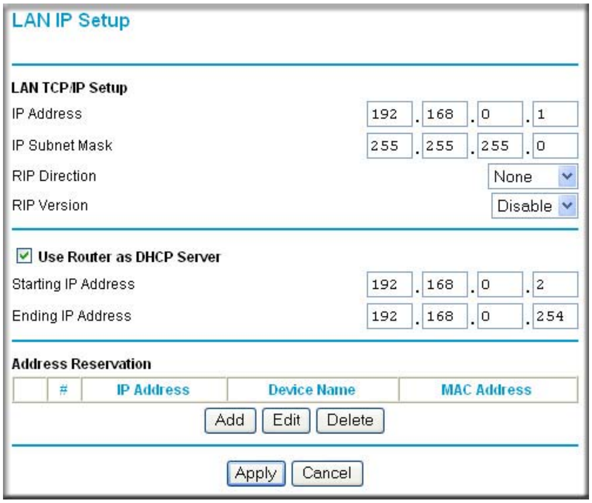
To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.

2. Click **Edit** or **Delete**.

How to Configure LAN TCP/IP Settings

1. Log in to the 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 User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu, under Advanced, click the LAN IP Setup link to view the menu, shown in Figure 6-3:



LAN IP Setup

LAN TCP/IP Setup

IP Address	192 . 168 . 0 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	None
RIP Version	Disable

☑ 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 6-3

3. Enter the TCP/IP, DHCP, or Reserved IP parameters.
4. Click **Apply** to save your changes.

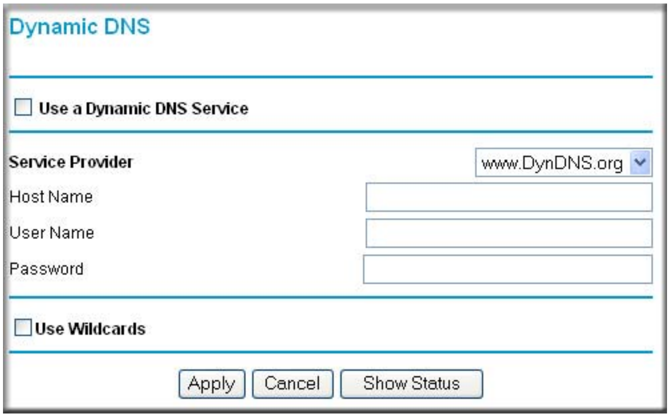
Configuring Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will 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 that will allow you to register your domain to their IP address, and will forward traffic directed at your domain to your frequently-changing IP address.

The router contains a client that can connect to a dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the router, whenever your ISP-assigned IP address changes, your router will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

How to Configure Dynamic DNS

1. Log in to the 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 User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, select Dynamic DNS to display the page below.



Dynamic DNS

□ Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name

User Name

Password

□ Use Wildcards

Figure 6-4

3. Access the Web site of one of the dynamic DNS service providers whose names appear in the ‘Service Provider’ box, and register for an account. For example, for dyndns.org, go to www.dyndns.org.
4. Select the **Use a dynamic DNS Service** check box.
5. Select the name of your dynamic DNS Service Provider.
6. Type the Host Name that your dynamic DNS service provider gave you. The dynamic DNS service provider may call this the domain name. If your URL is myName.dyndns.org, then your Host Name is “myName.”
7. Type the User Name for your dynamic DNS account.
8. Type the Password (or key) for your dynamic DNS account.

9. 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 will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org

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

> **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 will not be routed on the Internet

Using Static Routes

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

Static Route Example

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

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the wireless modem router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

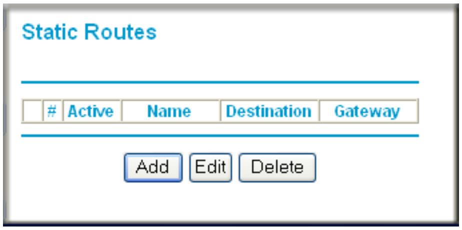
In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route setup would look like Figure 6-6.

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 Wireless Modem Router IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- The metric value represents the number of routers between your network and the destination. This is a direct connection so it can be set to the minimum value of 2.
- Private is selected only as a precautionary security measure in case RIP is activated.

How to Configure Static Routes

1. Log in to the 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 User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, click Static Routes to view the Static Routes menu, shown in Figure 6-5.

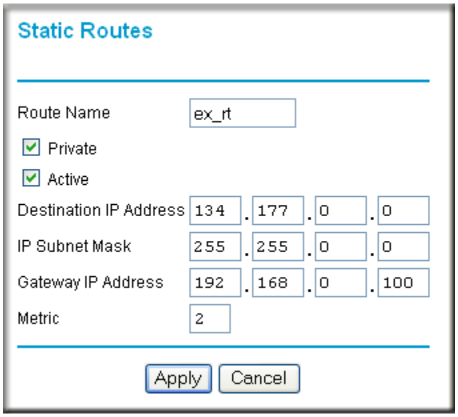


	#	Active	Name	Destination	Gateway

Figure 6-5

3. To add a Static Route:

a. Click the **Add** button to open the Edit Menu, shown in Figure 6-6.



Static Routes

Route Name: ex_rt

☑ Private

☑ Active

Destination IP Address: 134 . 177 . 0 . 0

IP Subnet Mask: 255 . 255 . 0 . 0

Gateway IP Address: 192 . 168 . 0 . 100

Metric: 2

Figure 6-6

b. Type a route name for this static route in the Route Name box under the table. This is for identification purpose only.

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

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

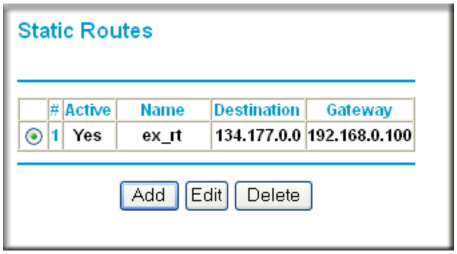
e. Type the Destination IP Address of the final destination.

f. Type the IP Subnet Mask for this destination. If the destination is a single host, type 255.255.255.255.

g. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.

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

4. Click **Apply**. The Static Routes table will update to show the new entry.



Static Routes

	#	Active	Name	Destination	Gateway
●	1	Yes	ex_rt	134.177.0.0	192.168.0.100

Figure 6-7

Chapter 7
Troubleshooting

This chapter gives information about troubleshooting your DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?
- Have I connected the router correctly?

  Go to "Basic Functioning" on page 7-1.

- I can't access the router's configuration with my browser.

  Go to "Troubleshooting the Web Configuration Interface" on page 7-3.

- I've configured the router but I can't access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 7-4.

- I can't remember the router's configuration password.
- I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 7-9.

Basic Functioning

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

1. When power is first applied, verify that the Power LED is on (see "The Router's Front Panel" on page 1-2 for an illustration and explanation of the LEDs).
2. After approximately 10 seconds, verify that:
   a. The Power LED is not red.
   b. The LAN port LEDs are lit for any local ports that are connected.
   c. The WAN port LED is lit.
   d. The Wireless LED is lit

If a port's LED is lit, a link has been established to the connected device. 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.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

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 12 V DC 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

When the router is turned on, it performs a power-on self test. If the Power LED turns red after a few seconds or at any other time during normal operation, there is a fault within the router. The power LED also turns red when you depress the factory default reset push button, and blinks red 3 times when that button is released. However, in this case, the wireless modem router is working normally.

If the power LED turns red to indicate a router fault:

- Cycle the power to see if the router recovers.

If the power LED is still red one minute after power up:

- 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 "Using the Reset button" on page 7-9.

If the error persists, you might have a hardware problem and should contact technical support.

LAN or Internet Port LEDs Not On

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

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.

- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
  - When connecting the router's Internet ADSL port, use the cable that was supplied with the DG834N.

Troubleshooting the Web Configuration Interface

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure 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. Follow the instructions in "Preparing a Computer for Network Access:" in Appendix B to configure your computer.

> **Note:** If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS will 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 "Using the Reset button" on page 7-9.
- 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 factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the router does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, 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.

Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should check the ADSL connection, then the WAN TCP/IP connection.

ADSL link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.

Internet LED Green or Blinking Green

If your Internet LED is green or blinking green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

Internet LED Blinking Amber

If your Internet LED is blinking amber, then your wireless modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the Internet LED does not turn green, 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.

If disconnecting telephones does not result in a green Internet LED, there may be a problem with your wiring. If the telephone company has tested the ADSL signal at your Network Interface Device (NID), then you may have poor quality wiring in your house.

Internet LED Off

If the Internet 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.

If disconnecting telephones does not result in a green Internet LED the problem may be one of the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It may be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The RangeMax NEXT Wireless ADSL2+ Modem Router uses pins 2 and 3.

Obtaining an Internet IP Address

If your wireless modem router is unable to access the internet, and your Internet LED is green or blinking green, you should determine whether the wireless modem router is able to obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your wireless modem router must request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

To check the Internet IP address from the browser interface:

1. Launch your browser and select an external site such as www.netgear.com.
2. Access the Main Menu of the wireless modem router’s configuration at http://192.168.0.1.
3. Under the Maintenance heading check that an IP address is shown for the WAN Port.
   If 0.0.0.0 is shown, your wireless modem router has not obtained an IP address from your ISP.

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

- If you have selected a login program, you may have incorrectly set the Service Name, User Name and Password. See “Troubleshooting PPPoE or PPPoA”, below.
- Your ISP may check for your computer's host name.
  Assign the computer Host Name of your ISP account to the wireless modem router in the browser-based Setup Wizard.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer’s MAC address. In this case:

Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

OR

Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu. Refer to *ADSL Modem Wireless Router Setup Manual*.

Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

1. Access the Main Menu of the router at http://192.168.0.1.
2. Under the Maintenance heading, select the Router Status link.
3. Click the Connection Status button.
4. If all of the steps indicate "OK" then your PPPoE or PPPoA connection is up and working.
5. If any of the steps indicates "Failed", you can attempt to reconnect by clicking "Connect". The wireless modem router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you may be using an incorrect Service Name, User Name or Password. There also may be a provisioning problem with your ISP.

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

Troubleshooting Internet Browsing

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

- Your computer may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the wireless modem router's configuration, reboot your computer and verify the DNS address as described in "Preparing a Computer for Network Access:" in Appendix B. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

  If your computer obtains its information from the wireless modem router by DHCP, reboot the computer and verify the wireless modem router address as described in "Preparing a Computer for Network Access:" in Appendix B.

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer.

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 PC running Windows 95 or later:

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

   ```
   ping 192.168.0.1
   ```

3. Click OK.

   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
     - Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or Internet Port LEDs Not On" on page 7-2.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.

- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

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

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

- Check that your PC has the IP address of your router listed as the default wireless modem router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC’s Network Control Panel. Verify that the IP address of the router is listed as the default wireless modem router as described in “Preparing a Computer for Network Access:” in Appendix B.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to “clone” or “spoof” the MAC address from the authorized PC. Refer to your *ADSL Modem Wireless Router Setup Manual*.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration 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 Web Configuration Manager (see "Backing Up, Restoring, or Erasing Your Settings" on page 5-1).
- Use the Default Reset 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 Reset button

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button until the Power LED turns red (about 5 seconds).
2. Release the Default Reset button. The LED will blink red three times and then turn green when the router has reset to the factory default state. Wait for the router to reboot.

Problems with Date and Time

The E-mail menu in the Content Filtering section displays the current date and time of day. The RangeMax NEXT Wireless ADSL2+ 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:

- Date shown is January 1, 2000
  Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour
  Cause: The router does not automatically sense Daylight Savings Time. In the E-mail menu, check or uncheck the box marked "Adjust for Daylight Savings Time".

Appendix A
Technical Specifications

This appendix provides technical specifications for the DG834N RangeMax™ NEXT Wireless ADSL2+ Modem Router.

General Specifications

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power Adapter	
North America:	120V, 60 Hz, input
UK, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
All regions (output):	12 V AC @ 1.0A output, 30W maximum
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
Environmental	
Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	10% to 90% relative humidity, noncondensing
Storage temperature:	-20° to 70° C (-4º to 158º F)
Storage humidity:	5 to 95% relative humidity, noncondensing
Regulatory Compliance	
Meets requirements of:	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B

Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	ADSL, Dual RJ-11, pins 2 and 3 T1.413, G.DMT, G.Lite ITU Annex A or B ITU G.992.5 (ADSL2+)

Default Configuration

You can use the reset button located on the front of your device to reset all settings to their factory defaults. This is called a hard reset. To perform a hard reset, push and hold the reset button for five seconds. Your device will return to the factory configuration settings shown in the table below.

Feature		**Default Behavior**
Router Login		
	User Login URL	http://www.routerlogin.net *or* http://www.routerlongin.com
	User Name (case sensitive)	admin
	Login Password (case sensitive)	password
Internet Connection		
	WAN MAC Address	Use Default address
	WAN MTU Size	1500
	Port Speed	AutoSense
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	Enabled or disabled

Feature		**Default Behavior**
	Time Zone	GMT
	Time Zone Adjusted for Daylight Saving Time	Disabled
	SNMP	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless		
	Wireless Communication	Enabled
	SSID Name	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	Country/Region	Europe
	RF Channel	6
	Operating Mode	Up to 270 Mbps* (with 20/40 MHz bandwidth dynamically selected on a frame-by-frame basis).
	Data Rate	Best
	Output Power	Full
	Access Point	Enabled
	Authentication Type	Open System
	Wireless Card Access List	All wireless stations allowed

*. 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.

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
Internet Networking and TCP/IP Addressing:	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications:	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access:	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN):	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary:	http://documentation.netgear.com/reference/enu/glossary/index.htm