

Reference Manual for the ADSL Modem Wireless Router DG834G

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10155-05
April 2007

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 modem router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Česky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento 54 Mbps ADSL Modem Wireless Router Model DG834G je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr 54 Mbps ADSL Modem Wireless Router Model DG834G overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät 54 Mbps ADSL Modem Wireless Router Model DG834G in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme 54 Mbps ADSL Modem Wireless Router Model DG834G vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this 54 Mbps ADSL Modem Wireless Router Model DG834G 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 54 Mbps ADSL Modem Wireless Router Model DG834G 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 54 Mbps ADSL Modem Wireless Router Model DG834G 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 54 Mbps ADSL Modem Wireless Router Model DG834G 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 54 Mbps ADSL Modem Wireless Router Model DG834G è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarā, ka 54 Mbps ADSL Modem Wireless Router Model DG834G atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis 54 Mbps ADSL Modem Wireless Router Model DG834G atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel 54 Mbps ADSL Modem Wireless Router Model DG834G 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 54 Mbps ADSL Modem Wireless Router Model DG834G jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a 54 Mbps ADSL Modem Wireless Router Model DG834G megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oświadczam, że 54 Mbps ADSL Modem Wireless Router Model DG834G jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este 54 Mbps ADSL Modem Wireless Router Model DG834G está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta 54 Mbps ADSL Modem Wireless Router Model DG834G v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že 54 Mbps ADSL Modem Wireless Router Model DG834G spáda základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että 54 Mbps ADSL Modem Wireless Router Model DG834G 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 DG834G v4 product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das 54 Mbps ADSL Modem Wireless Router Model DG834G 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 54 Mbps ADSL Modem Wireless Router Model DG834G 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 54 Mbps ADSL Modem Wireless Router Model DG834G.

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:	DG834G v4
Publication Date:	April 2007
Product Family:	Modem Router
Product Name:	54 Mbps ADSL Modem Wireless Router Model DG834G
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10155-05
Publication Version Number:	1.4

Contents

Reference Manual for the ADSL Modem Wireless Router DG834G

Chapter 1

About This Manual

Audience, Scope, Conventions, and Formats	1-1
How to Print this Manual	1-2

Chapter 2

Introduction

About the Modem Router	2-1
Key Features	2-2
A Powerful, True Firewall	2-2
802.11 Standards-based Wireless Networking	2-3
Easy Installation and Management	2-3
Protocol Support	2-4
Virtual Private Networking (VPN)	2-5
Auto Sensing and Auto Uplink™ LAN Ethernet Connections	2-5
Content Filtering	2-6
Wi-Fi Multimedia (WMM) Quality of Service (QoS)	2-6
Wireless Distribution System (WDS)	2-6
What's in the Box?	2-6
The Modem Router's Front Panel	2-8
The Modem Router's Rear Panel	2-9

Chapter 3

Configuring Your Internet Connection

Connecting the Router to the Internet	3-1
Manual Setup	3-1
What You Need Before You Begin	3-1
Understanding ADSL Microfilters	3-2
Computers Set to DHCP	3-3

Manually Setting Up Your Modem Router	3-4
Auto-Detecting Your Internet Connection Type	3-10
Wizard-Detected PPPoE Login Account Setup	3-11
Wizard-Detected PPPoA Login Account Setup	3-11
Wizard-Detected Dynamic IP Account Setup	3-12
Wizard-Detected IP Over ATM Account Setup	3-12
Wizard-Detected Fixed IP (Static) Account Setup	3-13
Testing Your Internet Connection	3-14
Manually Configuring Your Internet Connection	3-15
How to Perform Manual Configuration	3-16
ADSL Settings	3-20

Chapter 4

Wireless Configuration

Considerations for a Wireless Network	4-1
Observe Performance, Placement, and Range Guidelines	4-1
Implement Appropriate Wireless Security	4-2
Understanding Wireless Settings	4-4
How to Set Up and Test Basic Wireless Connectivity	4-7
How to Restrict Wireless Access to Your Network	4-8
Choosing WEP Authentication and Security Encryption Methods	4-11
How to Configure WEP	4-13
How to Configure WPA-PSK/WPA2-PSK Security	4-14
How to Configure WPA-802.1x/WPA2-802.1x Security	4-15

Chapter 5

Protecting Your Network

Protecting Access to Your 54 Mbps ADSL Modem Wireless Router Model DG834G	5-1
How to Change the Built-In Password	5-1
Changing the Administrator Login Timeout	5-2
Configuring Basic Firewall Services	5-3
Blocking Keywords, Sites, and Services	5-3
How to Block Keywords and Sites	5-3
Firewall Rules	5-5
Instant Messaging (IM) Ports	5-6
Inbound Rules (Port Forwarding)	5-7
Outbound Rules (Service Blocking)	5-10

Order of Precedence for Rules	5-12
Services	5-13
How to Define Services	5-13
Setting Times and Scheduling Firewall Services	5-14
How to Set Your Time Zone	5-14
How to Schedule Firewall Services	5-16

Chapter 6

Managing Your Network

Backing Up, Restoring, or Erasing Your Settings	6-1
How to Back Up the Configuration to a File	6-1
How to Restore the Configuration from a File	6-2
How to Erase the Configuration	6-2
Upgrading the Modem Router's Firmware	6-2
How to Upgrade the Modem Router Firmware	6-3
Network Management Information	6-4
Viewing Modem Router Status and Usage Statistics	6-4
Viewing Attached Devices	6-9
Viewing, Selecting, and Saving Logged Information	6-9
Examples of Log Messages	6-12
Enabling Security Event E-mail Notification	6-13
Running Diagnostic Utilities and Rebooting the Modem Router	6-15
Enabling Remote Management	6-16
Configuring Remote Management	6-16

Chapter 7

Advanced Configuration

Configuring Advanced Security	7-1
Setting Up A Default DMZ Server	7-2
Connect Automatically, as Required	7-3
Enable PPPoE-Relay	7-4
Disable Port Scan and DOS Protection	7-4
Respond to Ping on Internet WAN Port	7-4
MTU Size	7-4
Configuring LAN IP Settings	7-4
DHCP	7-6
How to Configure LAN TCP/IP Settings	7-8

Configuring Dynamic DNS	7-9
How to Configure Dynamic DNS	7-9
Using Static Routes	7-11
Static Route Example	7-11
How to Configure Static Routes	7-12
Universal Plug and Play (UPnP)	7-13
Wireless Bridging and Repeating	7-14
Point-to-Point Bridge Configuration	7-16
Multi-Point Bridge Configuration	7-17
Repeater with Wireless Client Association	7-19

Chapter 8

Virtual Private Networking

Overview of VPN Configuration	8-2
Client-to-Gateway VPN Tunnels	8-2
Gateway-to-Gateway VPN Tunnels	8-3
Planning a VPN	8-4
VPN Tunnel Configuration	8-6
How to Set Up a Client-to-Gateway VPN Configuration	8-7
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834G v4	8-7
Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC	8-12
How to Set Up a Gateway-to-Gateway VPN Configuration	8-21
VPN Tunnel Control	8-29
Activating a VPN Tunnel	8-29
Verifying the Status of a VPN Tunnel	8-33
Deactivating a VPN Tunnel	8-35
Deleting a VPN Tunnel	8-37
How to Set Up VPN Tunnels in Special Circumstances	8-38
Using Auto Policy to Configure VPN Tunnels	8-38
Using Manual Policy to Configure VPN Tunnels	8-48

Chapter 9

Troubleshooting

Basic Functioning	9-1
Power LED Not On	9-2
Test LED Never Turns On or Test LED Stays On	9-2
LAN or Internet Port LEDs Not On	9-2

Troubleshooting the Web Configuration Interface	9-3
Troubleshooting the ISP Connection	9-4
ADSL link	9-4
Obtaining a WAN IP Address	9-5
Troubleshooting PPPoE or PPPoA	9-6
Troubleshooting Internet Browsing	9-7
Troubleshooting a TCP/IP Network Using the Ping Utility	9-7
Testing the LAN Path to Your Router	9-7
Testing the Path from Your Computer to a Remote Device	9-8
Restoring the Default Configuration and Password	9-9
Using the Reset button	9-9
Problems with Date and Time	9-9

Appendix A
Technical Specifications

Appendix B
NETGEAR VPN Configuration

DG834G v4 to FVL328	B-1
Configuration Profile	B-1
Step-By-Step Configuration	B-2
DG834G v4 with FQDN to FVL328	B-6
Configuration Profile	B-6
Step-By-Step Configuration	B-8
Configuration Summary (Telecommuter Example)	B-14
Setting Up the Client-to-Gateway VPN Configuration (Telecommuter Example)	B-14
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office	B-15
Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office	B-18
Monitoring the VPN Tunnel (Telecommuter Example)	B-28
Viewing the PC Client's Connection Monitor and Log Viewer	B-28
Viewing the VPN Router's VPN Status and Log Information	B-29

Appendix C
Related Documents

Chapter 1

About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

Audience, Scope, Conventions, and Formats

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the Netgear website.



Note: Product updates are available on the NETGEAR, Inc. Web site at <http://kbserver.netgear.com/products/DG834G v4.asp>.

This guide uses the following typographical conventions:

Table 1-1.

<i>italics</i>	Emphasis, books, CDs, URL names
bold	User input
<code>fixed</code>	Screen text, file and server names, extensions, commands, IP addresses

This guide 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.

This manual is written for the ADSL Modem Wireless Router according to these specifications:

Table 1-2. Manual Scope

Product Version	54 Mbps ADSL Modem Wireless Router Model DG834G
Manual Publication Date	April 2007

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 the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at <http://www.adobe.com>.

- 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 2

Introduction

This chapter describes the features of the NETGEAR 54 Mbps ADSL Modem Wireless Router Model DG834G. The ADSL Modem Wireless Router is a combination of a built-in ADSL modem, modem router, 4-port switch, and firewall which enables your entire network to safely share an Internet connection that otherwise would be used by a single computer.



Note: If you are unfamiliar with networking and routing, refer to [“Internet Networking and TCP/IP Addressing”](#) in [Appendix C](#) to become more familiar with the terms and procedures used in this manual.

About the Modem Router

The 54 Mbps ADSL Modem Wireless Router Model DG834G provides continuous, high-speed 10/100 Ethernet access between your Ethernet devices. With minimum setup, you can install and use the modem router within minutes.

The ADSL Modem Wireless Router provides multiple Web content filtering options, reporting, and instant alerts. Parents and network administrators can establish restricted access policies based on time of day, Web site addresses, and address keywords. They can also share high-speed ADSL Internet access for up to 253 personal computers. The included firewall and Network Address Translation (NAT) features protect you from hackers.

Key Features

The ADSL Modem Wireless Router provides the following features:

- A built-in ADSL modem
- A powerful, true firewall
- 802.11g standards-based wireless networking
- Easy, Web-based setup for installation and management
- Extensive Internet protocol support
- Trustworthy VPN Communications over the Internet
- VPN Wizard for easy VPN configuration
- Auto Sensing and Auto Uplink™ LAN Ethernet connections
- Content filtering
- Wi-Fi Multimedia (WMM) QoS (Quality of Service) to prioritize voice and video traffic

These features are discussed below.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the DG834G v4 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- 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.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents
The DG834G v4 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the modem router to email the log to you at specified intervals. You can also configure the modem router to send immediate alert messages to your email address or email pager whenever a significant event occurs.

802.11 Standards-based Wireless Networking

The ADSL Modem Wireless Router includes an 802.11g-compliant wireless access point, providing continuous, high-speed 10/100 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11g Standards-based wireless networking at up to 54 Mbps
- Works with both 802.11g and 802.11b wireless devices
- 64-bit and 128-bit WEP encryption security
- WEP keys can be entered manually or generated by passphrase
- Support for Wi-Fi Protected Access Pre-Shared Key (WPA-PSK and WPA2-PSK) encryption and 802.1x authentication
- Wireless access can be restricted by MAC address

Easy Installation and Management

You can install, configure, and operate the DG834G v4 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**
Browser-based configuration allows you to easily configure your modem router from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **Smart Wizard**
The firmware in the modem router automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **Remote management**
The modem router allows you to log in to the Web management interface from a remote location via the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, or you can choose a nonstandard port number.
- **Diagnostic functions**
The modem router incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the modem router. You can use these diagnostic functions directly from the DG834G v4 when you are connected on the LAN or when you are connected over the Internet via the remote management function.

- Visual monitoring
The modem router's front panel LEDs provide an easy way to monitor its status and activity.
- Flash erasable programmable read-only memory (EPROM) for firmware upgrades.

Protocol Support

The DG834G v4 supports Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). [“Internet Networking and TCP/IP Addressing” in Appendix C](#) provides further information on TCP/IP.

- The Ability to Enable or Disable IP Address Sharing by NAT
The DG834G v4 allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account. This feature can also be turned off completely while using the DG834G v4 if you want to manage the IP address scheme yourself.
- Automatic Configuration of Attached PCs by DHCP
The DG834G v4 dynamically assigns network configuration information, including IP, modem router, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- DNS Proxy
When DHCP is enabled and no DNS addresses are specified, the modem router provides its own address as a DNS server to the attached PCs. The modem router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- Classical IP (RFC 1577)
Some Internet service providers, in Europe for example, use Classical IP in their ADSL services. In such cases, the modem router is able to use the Classical IP address from the ISP.
- PPP over Ethernet (PPPoE)
PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an ADSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your computer.
- PPP over ATM (PPPoA)
PPP over ATM is a protocol for connecting remote hosts to the Internet over an ADSL connection by simulating an ATM connection.

- Point-to-Point Tunneling Protocol (PPTP)
Typically used as a protocol for virtual private networks. This protocol is used by some Russian ISPs for connecting remote hosts to the Internet over an ADSL connection.



Note: PPTP must be manually configured. At present, the SmartWizard cannot automatically detect a PPTP type of connection with your ISP.

- Dynamic DNS
Dynamic DNS services allow remote users to find your network using a domain name when your IP address is not permanently assigned. The modem router contains a client that can connect to many popular Dynamic DNS services to register your dynamic IP address.
- Universal Plug and Play (UPnP)
UPnP is a networking architecture that provides compatibility between networking technologies. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

Virtual Private Networking (VPN)

The ADSL Modem Wireless Router provides a secure encrypted connection between your local area network (LAN) and remote networks or clients. It includes the following VPN features:

- Supports 5 VPN connections.
- Supports industry standard VPN protocols
The ADSL Modem Wireless Router supports standard Manual or IKE keying methods, standard MD5 and SHA-1 authentication methods, and standard DES and 3DES encryption methods. It is compatible with many other VPN products.
- Supports 3DES encryption for maximum security.
- VPN Wizard based on VPNC recommended settings.

Auto Sensing and Auto Uplink™ LAN Ethernet Connections

With its internal 4-port 10/100 switch, the DG834G v4 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The local LAN ports are autosensing and capable of full-duplex or half-duplex operation.

The modem router incorporates Auto Uplink™ technology. Each local Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a computer or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Content Filtering

With its content filtering feature, the DG834G v4 prevents objectionable content from reaching your PCs. The modem router allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the modem router to log and report attempts to access objectionable Internet sites.

Wi-Fi Multimedia (WMM) Quality of Service (QoS)

WMM is a QoS feature that provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must be WMM-enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best-effort category, which receives a lower priority than voice and video.

Wireless Distribution System (WDS)

WDS allows a wireless network to be expanded using access points, without needing a wired backbone to connect them. The DG834G v4 ADSL Modem Wireless Router can be configured to connect with other access points as a bridge (with wired clients only) or as a repeater (with wired and/or wireless clients).

What’s in the Box?

The product package should contain the following items:

- 54 Mbps ADSL Modem Wireless Router Model DG834G
- AC power adapter (varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector

- Microfilters (quantity and type vary by region)
- *DG834G ADSL Modem Wireless Router Resource CD*, including this guide
- Two plastic feet that can be used to stand the ADSL Modem Wireless Router on end
- 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 Modem Router's Front Panel

The front panel shown below contains status LEDs.

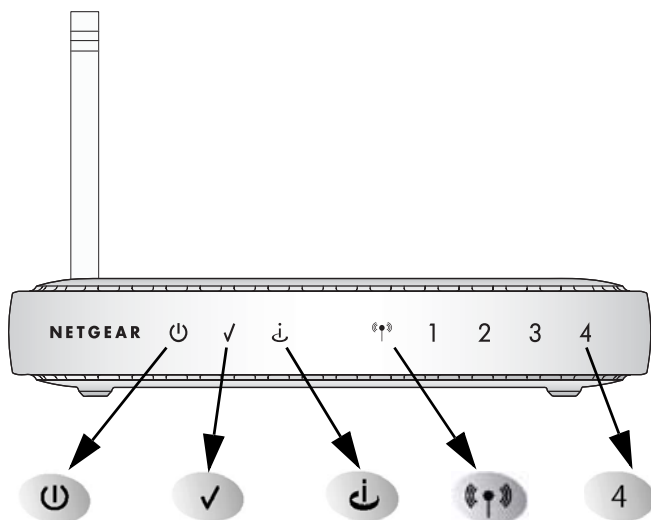


Figure 2-1

You can use the LEDs to verify various conditions. [Table 2-1](#) describes each LED.

Table 2-1. LED Descriptions

Label	Activity	Description
1. Power	On Off	Power is supplied to the router. Power is not supplied to the router.
2. Test	On Off	The system is initializing. The system is ready and running.
3. Internet	Blink -- Amber On -- Green Blink -- Green	Indicates ADSL training. The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
4. Wireless	On Off	Indicates that the Wireless port is initialized. 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 Modem Router's Rear Panel

The rear panel of the 54 Mbps ADSL Modem Wireless Router Model DG834G (Figure 2-2) contains port connections.

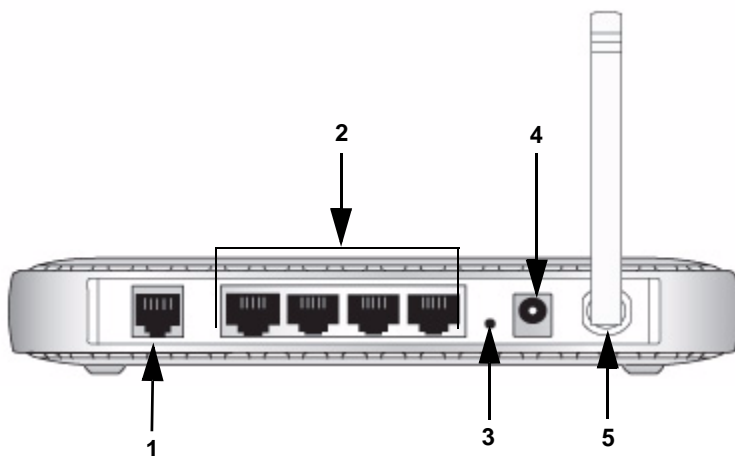


Figure 2-2

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

1. RJ-11 ADSL port for connecting the modem router to an ADSL line
2. Four Local Ethernet RJ-45 LAN ports for connecting the modem router to the local computers
3. Factory Default Reset push button
4. AC power adapter outlet
5. Wireless antenna

Chapter 3

Configuring Your Internet Connection

This chapter describes how to configure the wired internet connection of your 54 Mbps ADSL Modem Wireless Router Model DG834G.

Connecting the Router to the Internet

To connect your ADSL Modem Wireless Router to the Internet, refer to the *ADSL Modem Wireless Router Setup Manual* on the *DG834G ADSL Modem Wireless Router Resource CD* or online as shown in the following table.

Table 3-1.

Language	URL
Dutch	http://documentation.netgear.com/dg834g/nld/208-10039-01/
English	http://documentation.netgear.com/dg834g/enw/208-10033-01/
French	http://documentation.netgear.com/dg834g/fra/208-10034-01/
German	http://documentation.netgear.com/dg834g/dew/208-10035-01/
Italian	http://documentation.netgear.com/dg834g/ita/208-10036-01/
Spanish	http://documentation.netgear.com/dg834g/esp/208-10037-01/
Swedish	http://documentation.netgear.com/dg834g/sve/208-10038-01/

Manual Setup

Use the topics and procedures below to manually set up your modem router.

What You Need Before You Begin

You need to prepare the following before you can set up your modem router:

- Active Internet service provided by an ADSL account.

- The Internet Service Provider (ISP) configuration information for your ADSL account.
 - ISP Login Name and Password
 - ISP Domain Name Server (DNS) Addresses
 - Fixed or Static IP Address
- ADSL microfilters as explained below.
- Your computers set to DHCP.

Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it.

Internet Configuration Requirements

Depending on how your ISP set up your Internet account, you need one or more of these configuration parameters to connect your modem router to the Internet:

- Virtual Path Identifier (VPI)/Virtual Channel Identifier (VCI) parameters
- Multiplexing Method
- Host and Domain Names

Understanding ADSL Microfilters

ADSL technology uses the same wires as your telephone service. However, ADSL adds signals to the telephone lines which create noise in the telephone service. You must use ADSL microfilters to filter out these signals before they reach your telephone.




Note: If you purchased the modem router in a country where a microfilter is not included, you must acquire one.

ADSL Microfilter



Figure 3-1

Each device such as a telephone, fax machine, answering machine, or caller ID display will require an ADSL microfilter.

	<p>Warning: Do not connect the modem router to the ADSL line through a microfilter unless the microfilter is a combination microfilter/splitter specifically designed for this purpose. Doing so will prevent block your connection to the Internet. If you have any doubts about this, connect the modem router directly to the ADSL line.</p>
---	--

ADSL Microfilter with Built-In Splitter



Figure 3-2

Use an ADSL microfilter with built-in splitter when there is a single wall outlet which must provide connectivity for both the modem router and telephone equipment.

Computers Set to DHCP

For the initial connection to your modem router, your computer has to be set to automatically get its

TCP/IP configuration from the modem router via DHCP. This is usually the case. The NETGEAR Smart Wizard CD automatically takes care of this requirement. For manual setup, refer to the documentation that came with your computer.

Manually Setting Up Your Modem Router

There are four steps to setting up your modem router:

1. Install ADSL filters on the phone lines.
2. Connect the modem router to the ADSL line.
3. Log in to the modem router.
4. Connect to the Internet.

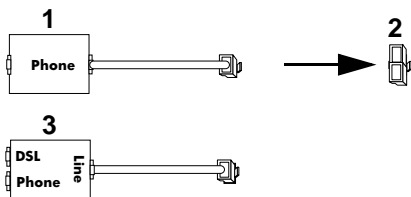
Follow the steps below to connect your modem router to your network. Before you begin, locate the ADSL configuration information from your Internet Service Provider (ISP).

1. Connect the ADSL filter.



Note: If you purchased the DG834G v4 in a country where an ADSL filter is not included, you must acquire one.

- a. You need to install an ADSL filter for every telephone that uses the same phone line as your modem router. Select the filter that came with your modem router.



1. One-Line Filter: Use with a phone or fax machine.
2. Splitter: Use with a one-line filter to share an outlet with a phone and the modem router.
3. Two-Line Filter with Splitter: Use to share an outlet with a phone and the modem router.

Figure 3-3

- b. **Two-Line Filter Example.** Insert the two-line filter into the phone outlet and connect the phone to the phone line connector (A):

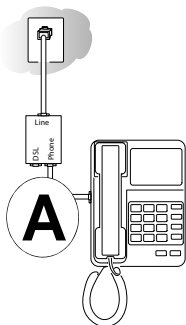


Figure 3-4



Note: To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

2. Connect the modem router to the ADSL filter.
 - a. Using the included phone cable with RJ-11 jacks, connect the ADSL port (**B**) of the modem router to the ADSL port (**C**) of the two-line filter.

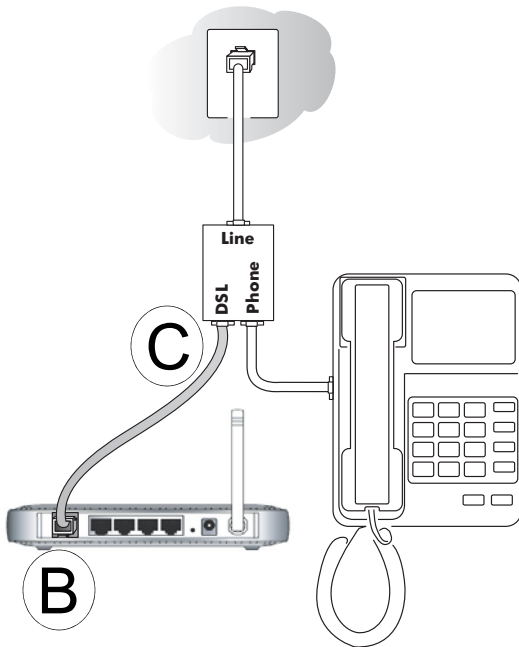


Figure 3-5

	<p>Warning: Improperly connecting a filter to your modem router will block your ADSL connection.</p>
--	---

- b. Connect the Ethernet cable (**D**) from a modem router LAN port to the Ethernet adapter in your computer.

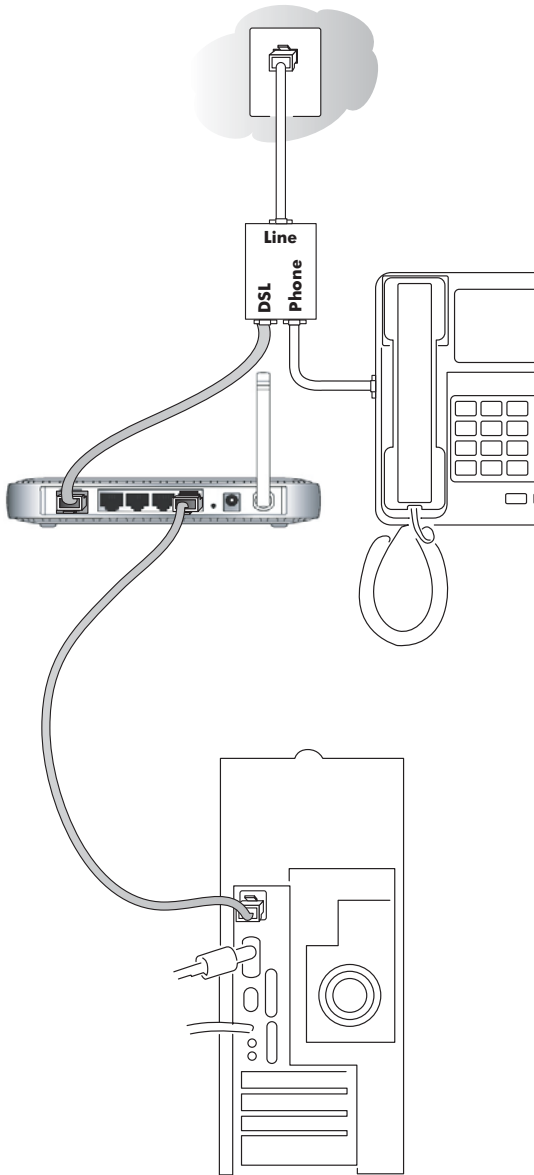








Figure 3-6

- c. Connect the power adapter to the modem router and plug it in to a power outlet. Verify the following:
 -  The power light is lit after turning on the modem router.
 -  The test light comes on briefly, then goes off.
 -  The wireless light is lit after turning on the modem router.
 -  The ADSL light is green, indicating you are connected to the ADSL network.
- d. Now, turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically. Verify the following:
 -  The local lights are lit for any connected computers.

3. Log in to the modem router.

	Note: Your computer needs to be configured for DHCP. For instructions on configuring for DHCP, please see the documentation that came with your computer or “Preparing a Computer for Network Access” in Appendix C.
---	---

- a. Type `http://Default IP Address Variable` in the address field of a browser such as Internet Explorer or Netscape® Navigator.



Figure 3-7

This login window opens:

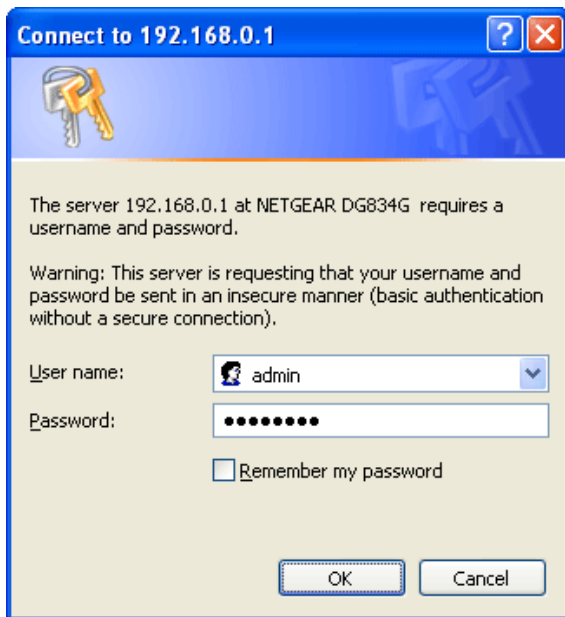


Figure 3-8

Enter **admin** for the user name and **password** for the password, both in lower case letters.

- b. After logging in, you will see the menu below.

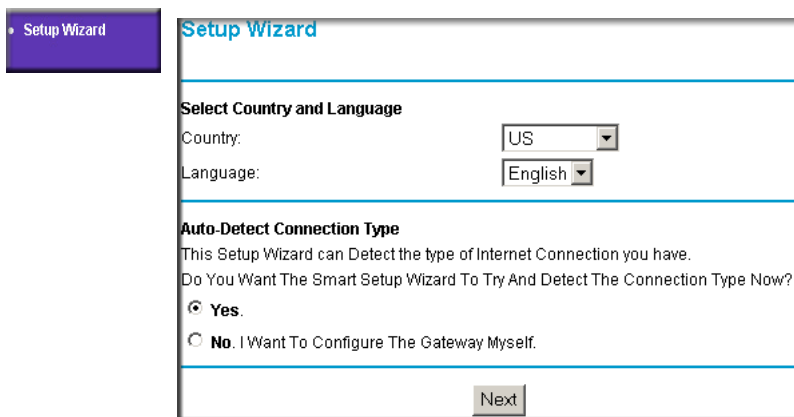


Figure 3-9

4. Connect to the Internet

You are now ready to configure your modem router to connect to the Internet. There are two ways you can configure your modem router to connect to the Internet:

- a. Let the modem router Setup Wizard auto-detect the type of Internet connection you have and configure it.
- b. Manually choose which type of Internet connection you have and configure it.

In either case, use the configuration parameters your ISP provided to assure that the configuration settings for your Internet connection are correct.

5. Test your Internet connection.

From the bottom of the Setup menu, click Test. If the NETGEAR Web site does not appear within one minute, refer to [Chapter 9, “Troubleshooting”](#).

Your modem router is now configured to provide Internet access for your network. Your modem router automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as Dial-Up Networking or Enternet to connect, log in, or disconnect. These functions are performed automatically by the modem router as needed.

To access the Internet from any computer connected to your modem router, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the modem router’s Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

Auto-Detecting Your Internet Connection Type

The Web Configuration Manager built in to the modem router contains a Setup Wizard that can automatically determine your network connection type.

The procedures for filling in the configuration page for each type of connection follow below.



Note: At present, the SmartWizard cannot automatically detect a PPTP type of connection with your ISP. If your ISP uses this type of protocol you must configure your connection manually (see [“Manually Setting Up Your Modem Router”](#) on [page 3-4](#)).

Wizard-Detected PPPoE Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over Ethernet (PPPoE), you will be directed to the PPPoE page shown:



Figure 3-10

Enter the PPPoE login user name and password.

Wizard-Detected PPPoA Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over ATM (PPPoA), you will be directed to the PPPoA page shown:



Figure 3-11

Enter your login user name and password. These fields are case sensitive.

Wizard-Detected Dynamic IP Account Setup

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the page shown:



Figure 3-12

Click Apply to set Dynamic IP as the connection method.

Wizard-Detected IP Over ATM Account Setup

If the Setup Wizard determines that your Internet service account uses IP over ATM Classical IP assignment (RFC1577), you will be directed to the page shown:



Figure 3-13

1. Enter your assigned IP Address and Subnet Mask. This information should have been provided to you by your ISP. You need the configuration parameters from your ISP.
2. Enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

DNS servers are required to perform the function of translating an Internet name such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here.

3. Click Apply to save the settings.
4. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to [Chapter 9, “Troubleshooting”](#).

Wizard-Detected Fixed IP (Static) Account Setup

If the router determines that your Internet service account uses Fixed IP assignment, you will be directed to the page where you can enter the IP addresses.

1. If required, enter the Account Name and Domain Name from your ISP.
2. Choose “Use Static IP Address” or “Use IP Over ATM” (IPoA — RFC1483 Routed) according to the information from your ISP. If you choose IPoA, the router will be able to detect the gateway IP address but you still need to provide the router IP address.
3. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP’s gateway modem router. This information should have been provided to you by your ISP. You need the configuration parameters from your ISP.
4. Enter the IP address of your ISP’s Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

DNS servers are required to perform the function of translating an Internet name such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here.

5. Click Apply to save the settings.
6. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to [Chapter 9, “Troubleshooting”](#).

Testing Your Internet Connection

After completing the Internet connection configuration, you can test your Internet connection. Log in to the modem router, then, from the Basic Settings link in the Setup menu, click the Test button. If the NETGEAR Web site does not appear within one minute, refer to [Chapter 9, “Troubleshooting”](#).

Your modem router is now configured to provide Internet access for your network. Your modem router automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as Dial-Up Networking or Enternet to connect, log in, or disconnect. These functions are performed by the modem router as needed.

To access the Internet from any computer connected to your modem router, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the modem router’s Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

The following chapters describe how to configure the Advanced features of your modem router, and how to troubleshoot problems that may occur.

Manually Configuring Your Internet Connection

You can manually configure your modem router using the menu below, or you can allow the Setup Wizard to determine your configuration as described in the previous section.

ISP Does Not Require Login

Basic Settings

Does Your Internet Connection Require A Login?

Yes

No

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

Get Dynamically From ISP

Use Static IP Address

IP Address . . .

IP Subnet Mask . . .

Gateway IP Address . . .

Use IP Over ATM (IPoA)

IP Address . . .

IP Subnet Mask . . .

Gateway IP Address . . .

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS . . .

Secondary DNS . . .

NAT (Network Address Translation)

Enable Disable Disable firewall

Router MAC Address

Use Default Address

Use Computer MAC Address

Use This MAC Address

Apply Cancel Test

ISP Does Require Login

Basic Settings

Does Your Internet Connection Require A Login?

Yes

No

Encapsulation

Login

Password

Idle Timeout (In Minutes)

Internet IP Address

Get Dynamically From ISP

Use Static IP Address

IP Address . . .

Domain Name Server (DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS . . .

Secondary DNS . . .

NAT (Network Address Translation)

Enable Disable Disable firewall

Apply Cancel Test

Figure 3-14

How to Perform Manual Configuration

We recommend that you start the manual configuration from the Setup Wizard:

1. Select your country and language. Language choices are English, French, German, and Italian. After you change the language, the remaining setup screens change to the language of your choice.
2. Select No to manually configure your modem router connection.
3. Click **Next**.
4. Manually configure the modem router in the Basic Settings menu shown above.
5. Follow the instructions below according to the encapsulation method and whether your Internet connection requires a login. The following methods are available:
 - Internet Connection Requires Login and Uses PPPoE
 - Internet Connection Requires Login and Uses PPPoA
 - Internet Connection Does Not Require a Login
6. Usually the default ADSL Settings work fine for most ISPs and you can skip this step. If you have any problems with your connection, check the ADSL Settings. See [“ADSL Settings” on page 3-20](#) for more details.

Internet Connection Requires Login and Uses PPPoE

1. If your Internet connection *does* require login, select Yes and fill in the settings according to the instructions below.



Note: 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 modem router automatically logs you in.

2. Choose PPPoE for the encapsulation method.
3. Enter the login name (frequently the email address your ISP provided), password, and service name (if required).
4. If you want to change the login timeout, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of zero means never log out.
5. When a connection uses PPPoE, the IP address is normally assigned automatically. However, the DG834G v4 allows this address to be set manually.

- Select “Get Dynamically from ISP” if your ISP assigns your IP address.
 - Select “Use Static IP Address” if your ISP gave you a statically assigned address.
6. The DNS server is used to look up site addresses based on their names.
- Select “Get Automatically from ISP” if your ISP uses DHCP to assign your DNS servers. Your ISP will automatically assign this address.
 - Select “Use These DNS Servers” if your ISP gave you one or two DNS addresses. Type the primary and secondary addresses.
7. You should only disable NAT if you are sure you do not require it. NAT automatically assigns private IP addresses (192.168.0.x) to LAN connected devices. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses the DG834G v4 uses. Classical routing should be selected only by experienced users.



Note: Disabling NAT will reboot the router and reset all the DG834G v4 configuration settings to the factory default. Disable NAT only if you plan to install the DG834G v4 in a setting where you will be manually administering the IP address space on the LAN side of the router.

The “Disable Firewall” option disables the firewall in addition to disabling NAT. The “Disable” option leaves the firewall active. With the firewall disabled, the protections normally provided to your network will be disabled.

Internet Connection Requires Login and Uses PPPoA

1. If your Internet connection *does* require login, select Yes and fill in the settings according to the instructions below.



Note: 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 modem router automatically logs you in.

2. Choose PPPoA for the encapsulation method.
3. Enter the login name (frequently the email address your ISP provided), and password.
4. If you want to change the login timeout, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of zero means never log out.

5. When a connection uses PPPoA, the IP address is normally assigned automatically. However, the DG834G v4 allows this address to be set manually.
 - Select “Get Dynamically from ISP” if your ISP assigns your IP address.
 - Select “Use Static IP Address” if your ISP gave you a statically assigned address.
6. The DNS server is used to look up site addresses based on their names.
 - Select “Get Automatically from ISP” if your ISP uses DHCP to assign your DNS servers. Your ISP will automatically assign this address.
 - Select “Use These DNS Servers” if your ISP gave you one or two DNS addresses. Type the primary and secondary addresses. You should only disable NAT if you are sure you do not require it.
7. NAT automatically assigns private IP addresses (192.168.0.x) to LAN-connected devices. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses the DG834G v4 uses. Classical routing should be selected only by experienced users.



Note: Disabling NAT will reboot the router and reset all the DG834G v4 configuration settings to the factory default. Disable NAT only if you plan to install the DG834G v4 in a setting where you will be manually administering the IP address space on the LAN side of the router.

The “Disable Firewall” option disables the firewall in addition to disabling NAT. The “Disable” option leaves the firewall active. With the firewall disabled, the protections normally provided to your network will be disabled.

Internet Connection Requires Login and Uses PPTP

1. If your Internet connection *does* require login, select Yes and fill in the settings according to the instructions below.



Note: 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 modem router automatically logs you in.

2. Choose PPTP Client for the encapsulation method.
3. Set the following items using the information assigned to you by your ISP:
 - Your local IP address and IP subnet mask
 - The server IP address for your ISP

- Your user name and password

Internet Connection Does Not Require A Login

1. If your Internet connection does *not* require a login, select No and fill in the settings according to the instructions below.
2. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's mail or news servers.
3. Internet IP Address:
 - Select "Get Dynamically from ISP" if your ISP uses DHCP to assign your IP address. Your ISP will automatically assign these addresses.
 - Select "Use Static IP Address" if your ISP has assigned you a permanent, fixed (static) IP address. Enter the IP address that your ISP assigned. Also enter the IP Subnet Mask and the Gateway IP Address. The gateway is the ISP's modem router to which your modem router will connect.
 - Select "IP Over ATM (IPoA)" if your ISP uses Classical IP Addresses (RFC1577). Enter the IP address, IP Subnet Mask, and Gateway IP Addresses that your ISP assigned.
4. Domain Name Server (DNS) Address:
 - Select "Get Dynamically from ISP" if your ISP uses DHCP to assign your IP address. Your ISP will automatically assign this address.
 - If you know that your ISP does not automatically transmit DNS addresses to the modem 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.

A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your modem router during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here.
5. You should only disable NAT if you are sure you do not require it. NAT automatically assigns private IP addresses (192.168.0.x) to LAN connected devices. When NAT is disabled, only standard routing is performed by this router.

Classical routing lets you directly manage the IP addresses the DG834G v4 uses. Classical routing should be selected only by experienced users.



Note: Disabling NAT will reboot the router and reset all the DG834G v4 configuration settings to the factory default. Disable NAT only if you plan to install the DG834G v4 in a setting where you will be manually administering the IP address space on the LAN side of the router.

6. NAT automatically assigns private IP addresses (192.168.0.x) to LAN-connected devices. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses the DG834G v4 uses. Classical routing should be selected only by experienced users.

The “Disable Firewall” option disables the firewall in addition to disabling NAT. The “Disable” option leaves the firewall active. With the firewall disabled, the protections normally provided to your network will be disabled.

7. Modem Router MAC Address:

This section determines the Ethernet MAC address that will be used by the modem router 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 modem router to masquerade as that computer by “cloning” its MAC address.

To change the MAC address, select “Use this Computer’s MAC address”. The modem 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. Alternatively, select “Use this MAC address” and enter it.

8. Click **Apply** to save your settings.
9. Click **Test** to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to [Chapter 9, “Troubleshooting”](#).

ADSL Settings

The default settings of your 54 Mbps ADSL Modem Wireless Router Model DG834G will work fine for most ISPs. However, some ISPs use a specific Multiplexing Method and Virtual Circuit Number for the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI).



Note: The correct country must be selected from the Setup Wizard’s first page for the default ADSL Settings to work.

If your ISP provided you with a specific Multiplexing Method or VPI/VCI number, then fill in the following:

1. Select the ADSL Settings link from the main menu.
2. For the Multiplexing Method, select LLC-based or VC-based.
3. Type a number between 0 and 255 for the VPI. The default is 8.

4. Type a number between 1 and 65535 for the VCI. The default is 35.
5. Click **Apply**.

Chapter 4

Wireless Configuration

This chapter describes how to configure the wireless features of your 54 Mbps ADSL Modem Wireless Router Model DG834G.

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 modem router in order to maximize the network speed.

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 modem router. 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 modem router:

- Near the center of the area in which your computers will operate
- In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls)
- Away from sources of interference, such as computers, microwaves, and cordless phones
- With the Antenna tight and in the upright position
- 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 802.11g wireless networks at a maximum range of up to 300 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 ADSL Modem Wireless Router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

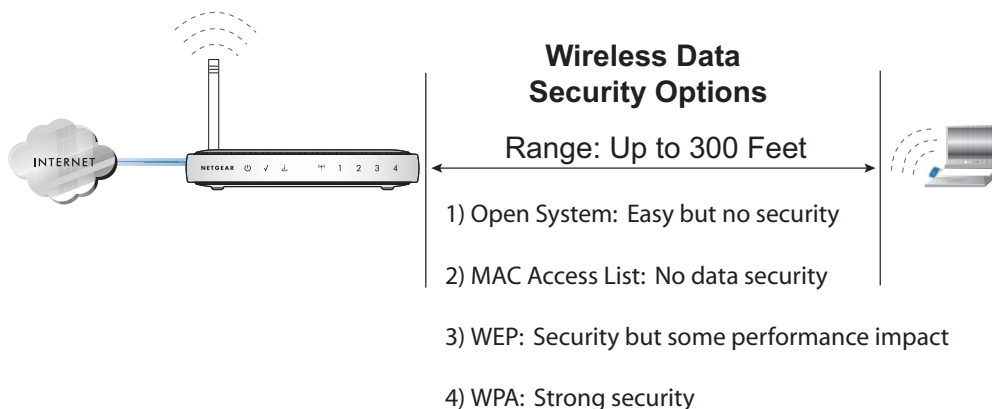


Figure 4-1

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 DG834G v4. 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.
- **WPA-802.1x, WPA2-802.1x.** Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and RADIUS servers.
- **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.

Understanding Wireless Settings

To configure the Wireless interface of your modem router, click the **Wireless Settings** link in the Setup section of the main menu. The Wireless Settings menu will appear, similar to that shown below:

Wireless Settings

Wireless Network

Name (SSID):

Region:

Channel:

Mode:

Wireless Access Point

Enable Wireless Access Point

Allow Broadcast of Name (SSID)

Wireless Isolation

Wireless Station Access List

Security Options

Disable

WEP (Wired Equivalent Privacy)

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

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

WPA-PSK+WPA2-PSK

WPA-802.1x

WPA2-802.1x


WPA-802.1x+WPA2-802.1x

Figure 4-2


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.

	Note: This value is case sensitive. For example, Wireless is not the same as wireless .
---	--

- **Region.** Select your country/region from the drop-down list. This field displays the region of operation for which the wireless interface is intended.

	Note: In the USA, the Region is preset according to regulatory requirements and cannot be changed. In other areas, you can and must set the Region. It may not be legal to operate the wireless access point in a region other than one of those identified in this field.
---	---

- **Channel.** 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 access point.
- **Mode.** The default is "g & b", which allows both "g" and "b" wireless stations to access this device. "g only" allows only 802.11g wireless stations to be used. "b only" allows 802.11b wireless stations; 802.11g wireless stations can still be used if they can operate in 802.11b mode.

- **Wireless Access Point.**

- **Enable Wireless Access Point.** This field lets you turn off or turn on the wireless access point built in to the modem router. The wireless icon on the front of the modem router will also 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 4-1. Wireless Security Options

Field	Description
<p>Disable</p> <p>WEP (Wired Equivalent Privacy)</p>	<p>Wireless security is not used.</p> <p>You can select the following WEP options:</p> <p>Authentication Type</p> <ul style="list-style-type: none"> • Open: the DG834G v4 does not perform any authentication. • Shared: WEP shared key authentication. For a full explanation of WEP shared key, see “Wireless Communications” in Appendix C. <p>Encryption Strength</p> <ul style="list-style-type: none"> • If Shared or Open Network Authentication is enabled, you can choose 64- or 128-bit WEP data encryption. <p>Note: With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the DG834G v4 <i>does</i> perform 64- or 128-bit data encryption but <i>does not</i> perform any authentication.</p> <p>Security Encryption (WEP) Key</p> <p>These key values must be identical on all wireless devices in your network (key 1 must be the same for all, key 2 must be the same for all, and so on). The DG834G v4 provides two methods for creating WEP encryption keys:</p> <ul style="list-style-type: none"> • Passphrase. These characters <i>are</i> case sensitive. Enter a word or group of printable characters in the Passphrase box and click the Generate button. <p>Note: Not all wireless adapters support passphrase key generation.</p> <ul style="list-style-type: none"> • Manual. These values <i>are not</i> case sensitive. <ul style="list-style-type: none"> 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).

Table 4-1. Wireless Security Options (continued)

Field	Description
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-PSK (AES) implements the full standard, but will not work with some older network cards. For a full explanation of WPA, see “Wireless Communications” in Appendix C .
WPA-802.1x, WPA2-802.1x	User authentication is implemented using 802.1x and RADIUS servers. For a full explanation of WPA, see “Wireless Communications” in Appendix C . Fill in the following: <ul style="list-style-type: none"> • Radius Server Name/IP Address This field is required. Enter the name or IP address of the Radius Server on your LAN. • Radius Port Enter the port number used for connections to the Radius Server. • Radius Shared Key Enter the desired value for the Radius shared key. This key enables the DG834G v4 to log in to the Radius server and must match the value used on the Radius server.

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 DG834G v4 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 DG834G v4 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 54 Mbps ADSL Modem Wireless Router Model DG834G. If they do not match, you will not get a wireless connection to the DG834G v4.

4. Set the Region. Select the region in which the wireless interface will operate.

5. Set the Channel. The default channel is 11.

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 modem router. For more information on the wireless channel frequencies please refer to [“Wireless Communications” in Appendix C](#).

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 “Disabled.”
7. Click **Apply** to save your changes.



Note: If you are configuring the modem router from a wireless computer and you change the modem router’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 modem router’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 modem router.

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

How to Restrict 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 54 Mbps ADSL Modem Wireless Router Model DG834G 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.

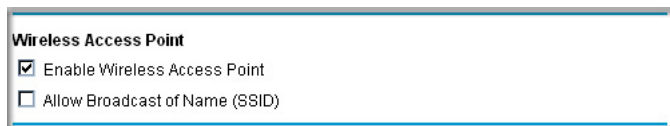


Figure 4-3

Restricting Access to Your Network by Turning Off Wireless Connectivity

You can completely turn off the wireless portion of the DG834G v4. 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 DG834G v4 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 DG834G v4. You must configure your wireless devices to match the wireless network name (SSID) you configure in the ADSL Modem Wireless Router.



Note: The SSID of any wireless access adapters must match the SSID you configure in the 54 Mbps ADSL Modem Wireless Router Model DG834G. If they do not match, you will not get a wireless connection to the DG834G v4.

Restricting Wireless Access Based on the Wireless Station Access List

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

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

1. Log in to the DG834G v4 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.

- 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

Delete

Available Wireless Stations

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

Add

Add New Station Manually

Device Name:

MAC Address:

Add

Apply Cancel

Figure 4-4

- Select the **Turn Access Control On** check box to enable restricting wireless computers by their MAC addresses.
- 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.
- 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 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**.

You can copy and paste the MAC addresses from the 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 modem router. The computer should then appear in the Attached Devices menu.



Note: If you are configuring the 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 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 DG834G v4. This prevents unauthorized access to your network.

Choosing WEP Authentication and Security Encryption Methods

Security Encryption (WEP)

Authentication Type:

Encryption Strength:

Security Encryption (WEP) Key

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

Figure 4-5

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 DG834G v4 lets you select the following wireless authentication schemes.

- Automatic
- Open System
- Shared key



Note: The authentication scheme is separate from the data encryption. You can choose an authentication scheme which requires a shared key but still leave the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

Set your wireless adapter according to the authentication scheme you choose for the ADSL Modem Wireless Router. Please refer to [“Wireless Communications” in Appendix C](#) for a full explanation of each of these options, as defined by the IEEE 802.11g wireless communication standard.

Encryption Choices

Please refer to [“Wireless Communications” in Appendix C](#) 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:

Disable. No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.

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:

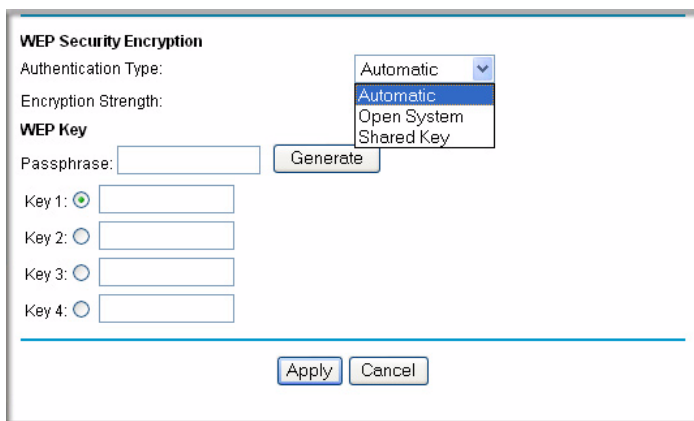
- **Passphrase.** Enter a word or group of printable characters in the Passphrase box and click the **Generate** button.
- **Manual.** 64-bit WEP: Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F).
128-bit WEP: Enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

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 DG834G v4 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 Setup section of the main menu for the DG834G v4 modem router.
3. In the Security Options section, select the **WEP (Wired Equivalent Privacy)** radio button
4. Go to the WEP Security Encryption portion of the page:



WEP Security Encryption

Authentication Type:

Encryption Strength:

WEP Key

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

Figure 4-6

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 DG834G v4.
9. Click **Apply** to save your settings.



Note: When configuring the 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 modem router WEP settings or access the modem router from a wired computer to make any further changes.

How to Configure WPA-PSK/WPA2-PSK Security



Note: Not all wireless adapters support WPA. Consult the product document for your wireless adapter for instructions on configuring WPA settings.

To configure WPA-PSK or 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 DG834G v4.
3. Choose the **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK+WPA2-PSK** radio button. The **WPA-PSK+WPA2-PSK** option is the most flexible, as it allows wireless clients to use either WPA-PSK or WPA2-PSK protocol. The Security Encryption section will be displayed.
4. Enter the pre-shared key in the Passphrase field.

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

How to Configure WPA-802.1x/WPA2-802.1x Security



Note: Not all wireless adapters support WPA. Consult the product document for your wireless adapter for instructions on configuring WPA settings.

To configure WPA-802.1x/WPA2-802.1x, 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 DG834G v4.
3. Choose the **WPA-802.1x**, **WPA2-802.1x**, or **WPA-802.1x+WPA2-802.1x** radio button. The **WPA-802.1x+WPA2-802.1x** option is the most flexible, as it allows wireless clients to use either WPA-802.1x or WPA2-802.1x protocol. The page will display the WPA-802.1x/WPA2-802.1x section.
4. Enter the Radius server name/IP address.
5. Enter the Radius port number.
6. Enter the Shared Key.
7. Click **Apply** to save your settings.

Chapter 5

Protecting Your Network

This chapter describes how to use the basic firewall features of the 54 Mbps ADSL Modem Wireless Router Model DG834G to protect your network.

Protecting Access to Your 54 Mbps ADSL Modem Wireless Router Model DG834G

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

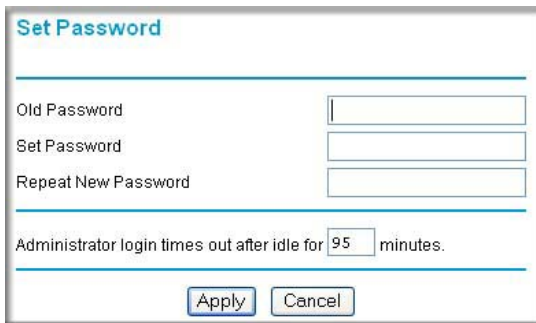
How to Change the Built-In Password

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



Figure 5-1


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



The screenshot shows a web form titled "Set Password". It contains three input fields: "Old Password", "Set Password", and "Repeat New Password". Below these fields is a label "Administrator login times out after idle for" followed by a text input field containing the number "95" and the word "minutes.". At the bottom of the form are two buttons: "Apply" and "Cancel".

Figure 5-2

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

	<p>Note: After changing the password, you will be required to log in again to continue the configuration. If you have backed up the modem router settings previously, you should do a new backup so that the saved settings file includes the new password.</p>
---	--

Changing the Administrator Login Timeout

For security, the administrator's login to the 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 modem router provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the ADSL Modem Wireless Router prevents objectionable content from reaching your PCs. The 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 modem router to perform these functions.

How to Block Keywords and Sites

The ADSL Modem Wireless 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 modem router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.

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

Block Sites

Keyword Blocking

Never

Per Schedule

Always

Type Keyword or Domain Name Here.

Add Keyword

Block Sites Containing these Keywords or Domain Names:

Delete Keyword Clear List

Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address ...

Apply Cancel

Figure 5-3

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 DG834G v4 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 5-12](#) for more details.

To access the rules configuration of the DG834G v4, 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

Add Edit Move Delete

Inbound Services

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

Add Edit Move Delete

Instant Messaging (IM) Ports

Close IM Ports

Open IM Ports (IM ports are open by default)

Apply Cancel

Figure 5-4

- 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**.

Instant Messaging (IM) Ports

In addition to the handling of rules for inbound and outbound services, the Firewall Rules menu provides options for the handling of instant messaging (IM) ports. By default, IM ports are open. If you select the **Close IM Ports** option, instant messaging will be effectively disabled on your local area network.

Inbound Rules (Port Forwarding)

Because the DG834G v4 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 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:

The screenshot shows the 'Inbound Services' configuration window. It contains the following fields and values:

- 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

At the bottom of the window are three buttons: Back, Apply, and Cancel.

Figure 5-5

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 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 which matches the parameters and action will be logged.
 - **Not match** — traffic of this type which does not match the parameters and action will be logged.

Inbound Rule Example: Allowing Videoconferencing

If you want to allow incoming videoconferencing 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 here, 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.

The screenshot shows the 'Inbound Services' configuration window. The 'Service' dropdown is set to 'CU-SEEME(TCP/UDP:7648)'. The 'Action' dropdown is set to 'ALLOW always'. The 'Send to LAN Server' field contains the IP address '192.168.0.11'. The 'WAN Users' dropdown is set to 'Address Range'. Below it, the 'start' field is '134.177.88.1' and the 'finish' field is '134.177.88.254'. The 'Log' dropdown is set to 'Not Match'. At the bottom, there are three buttons: 'Back', 'Apply', and 'Cancel'.

Figure 5-6

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 above). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The DG834G v4 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 modem router log any attempt to use Instant Messenger during that blocked period.

The screenshot shows the 'Outbound Services' configuration window. It has a title bar 'Outbound Services' and a blue header. Below the header, there are several sections:

- Service:** A dropdown menu with 'AIM(TCP:5190)' selected.
- Action:** A dropdown menu with 'BLOCK by schedule, otherwise allow' selected.
- LAN users:** A dropdown menu with 'Any' selected. Below it are 'start' and 'finish' fields, each with four input boxes for IP address digits.
- WAN Users:** A dropdown menu with 'Any' selected. Below it are 'start' and 'finish' fields, each with four input boxes for IP address digits.
- Log:** A dropdown menu with 'Match' selected.

At the bottom of the window are three buttons: 'Back', 'Apply', and 'Cancel'.

Figure 5-7

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; see [“How to Define Services” on page 5-13](#) for details.
- **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:

Outbound Services							
	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
<input type="radio"/>	1	<input checked="" type="checkbox"/>	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Move"/> <input type="button" value="Delete"/>							
Inbound Services							
	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
<input checked="" type="radio"/>	1	<input checked="" type="checkbox"/>	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
<input type="radio"/>	2	<input checked="" type="checkbox"/>	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Move"/> <input type="button" value="Delete"/>							

Figure 5-8

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 DG834G v4 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 modem router at its default LAN address of `http://192.168.0.1` with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.
2. Select the **Services** link of the Security menu to display the Services menu shown:



Figure 5-9

- 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.

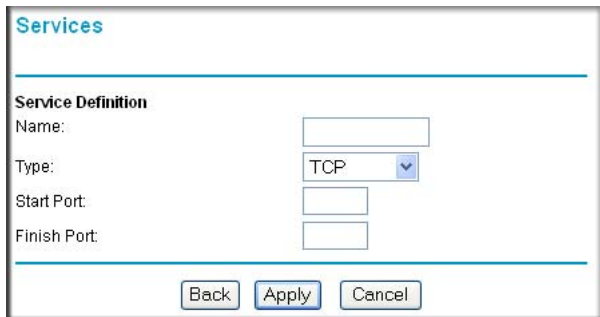


Figure 5-10

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

Setting Times and Scheduling Firewall Services

The ADSL Modem Wireless 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 modem router at its default LAN address of `http://192.168.0.1` with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.

2. Select the **Schedule** link of the Security menu to display menu shown below.

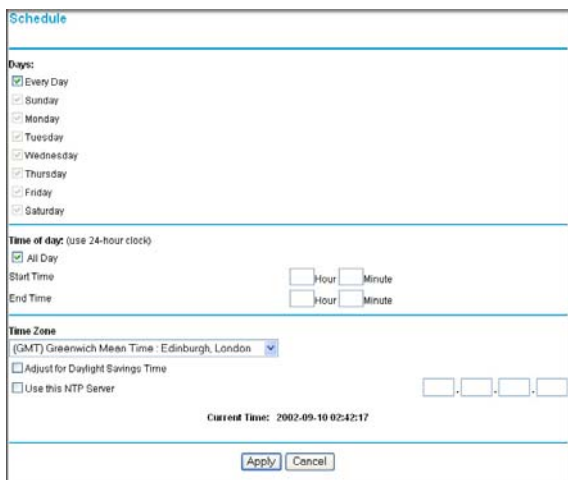


Figure 5-11

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 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 modem router at its default LAN address of `http://192.168.0.1` with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.
2. Select the **Schedule** link of the Security menu to display menu shown above.
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.
4. 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.
5. Click **Apply** to save your changes.

Chapter 6

Managing Your Network

This chapter describes how to perform network management tasks with your 54 Mbps ADSL Modem Wireless Router Model DG834G.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the ADSL Modem Wireless Router are stored in a configuration file in the 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 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 modem router.
2. From the Maintenance heading of the Main Menu, select the **Backup Settings** menu shown.

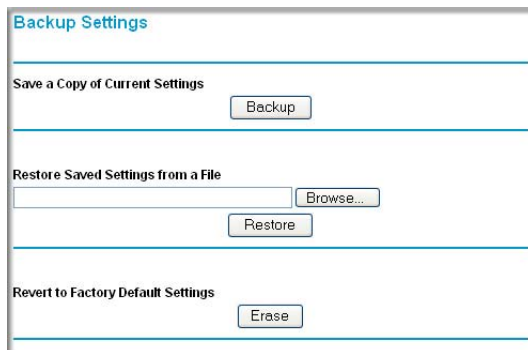


Figure 6-1

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 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 modem router.
2. From the Maintenance heading of the Main Menu, select the **Settings Backup** menu.
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 modem router.
5. The modem router will then reboot automatically.

How to Erase the Configuration

It is sometimes desirable to restore the 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 modem router will then reboot automatically.

After an erase, the modem router's password will be **password**, the LAN IP address will be 192.168.0.1, and the 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 modem router. See [“The Modem Router’s Rear Panel” on page 2-9](#).

Upgrading the Modem Router’s Firmware

The software of the ADSL Modem Wireless 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 modem router.

How to Upgrade the Modem Router Firmware

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 modem router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or above, or Netscape Navigator 4.7 or above.

2. Log in to the modem router at its default LAN address of `http://192.168.0.1` with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the 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.

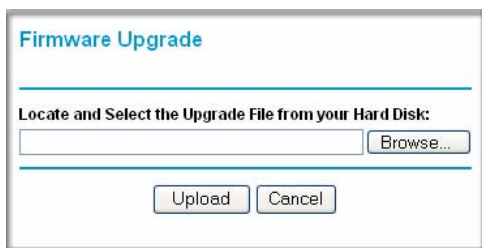


Figure 6-2

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



Warning: When uploading software to the 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 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 modem router after upgrading.

Network Management Information

The DG834G v4 provides a variety of status and usage information which is discussed below.

Viewing Modem Router Status and Usage Statistics

From the Main Menu, under Maintenance, click **Router Status** to view this screen.

The screenshot displays the 'Router Status' page with the following information:

Router Status	
<hr/>	
Account Name	
Firmware Version	V3.01.25
<hr/>	
ADSL Port	
MAC Address	00:0f:b5:c6:0e:91
IP Address	---
Network Type	PPPoE
IP Subnet Mask	---
Gateway IP Address	---
Domain Name Server	---
<hr/>	
LAN Port	
MAC Address	00:0f:b5:c6:0e:90
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
<hr/>	
Modem	
ADSL Firmware Version	4.01.02.00
Modem Status	Connecting
DownStream Connection Speed	0 kbps
UpStream Connection Speed	0 kbps
VPI	0
VCI	35
<hr/>	
Wireless Port	
Name (SSID)	zztopgun
Region	USA
Channel	11
Wireless AP	Enabled
Broadcast Name	Enabled
<hr/>	
<input type="button" value="Show Statistics"/> <input type="button" value="Connection Status"/>	

Figure 6-3

The Modem Router Status menu provides status and usage information.

This screen shows the following parameters:

Table 6-1. Menu 3.2 - Modem Router Status Fields

Field	Description
Account Name	The Host Name assigned to the modem router in the Basic Settings menu.
Firmware Version	This field displays the modem router firmware version.
ADSL Port	These parameters apply to the Internet (ADSL) port of the modem router.
MAC Address	This field displays the Ethernet MAC address being used by the Internet (ADSL) port of the modem router.
IP Address	This field displays the IP address being used by the Internet (ADSL) port of the modem router. If no address is shown, the modem router cannot connect to the Internet.
Network Type	The network type depends is determined by your ISP. Common network types are PPPoE and PPPoA.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (ADSL) port of the modem router.
Domain Name Server (DNS)	This field displays the DNS Server IP addresses being used by the modem router. These addresses are usually obtained dynamically from the ISP.
LAN Port	These parameters apply to the Local (ADSL) port of the modem router.
MAC Address	This field displays the Ethernet MAC address being used by the Local (LAN) port of the modem router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the modem router. The default is 192.168.0.1.
DHCP	If OFF, the modem router will not assign IP addresses to PCs on the LAN. If ON, the 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 modem router. The default is 255.255.255.0.
Modem	These parameters apply to the Local (WAN) port of the modem router.
ADSL Firmware Version	The version of the firmware.
Modem Status	The connection status of the modem.

Table 6-1. Menu 3.2 - Modem Router Status Fields (continued)

Field	Description
Downstream Speed	The speed at which the modem is receiving data from the ADSL line.
Upstream 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 4 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 DG834G v4 is configured to broadcast its SSID.

Click the **Show Statistics** button to display modem router usage statistics, as shown below:

System Up Time 00:08:51							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoE	0	0	0	0	0	00:00:00
LAN	10M/100M	542	751	0	294	155	00:08:47
WLAN	54M	288	0	0	70	0	00:08:36

ADSL Link	Downstream	Upstream
Connection Speed	0 kbps	0 kbps
Line Attenuation	0 db	0 db
Noise Margin	0 db	0 db

Poll Interval: (secs)

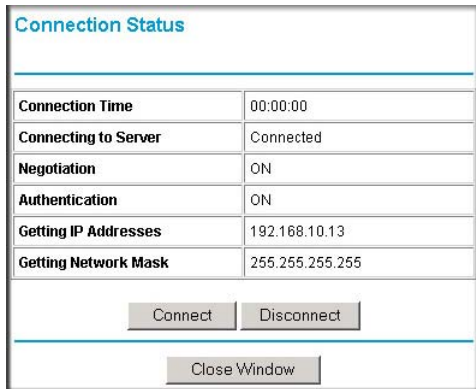
Figure 6-4

This screen shows the following statistics:

Table 6-2. Router Statistics Fields

Field	Description
WAN or LAN Port	The statistics for the WAN (Internet) and LAN ports.
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 modem router connection status, shown below:



The screenshot shows a window titled "Connection Status" with a table of connection details and three buttons: "Connect", "Disconnect", and "Close Window".

Connection Status	
Connection Time	00:00:00
Connecting to Server	Connected
Negotiation	ON
Authentication	ON
Getting IP Addresses	192.168.10.13
Getting Network Mask	255.255.255.255

Buttons: Connect, Disconnect, Close Window

Figure 6-5

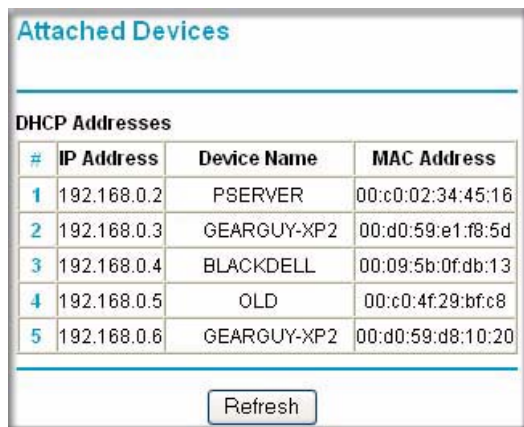
This screen shows the following statistics:

Table 6-3. Connection Status Fields for PPPoA

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	ON or OFF
Authentication	ON or OFF
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 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:



The screenshot shows a web interface titled "Attached Devices". Below the title is a table with the heading "DHCP Addresses". The table has four columns: "#", "IP Address", "Device Name", and "MAC Address". There are five rows of data. Below the table is a "Refresh" button.

#	IP Address	Device Name	MAC Address
1	192.168.0.2	PSEVER	00:c0:02:34:45:16
2	192.168.0.3	GEARGUY-XP2	00:d0:59:e1:f8:5d
3	192.168.0.4	BLACKDELL	00:09:5b:0f:db:13
4	192.168.0.5	OLD	00:c0:4f:29:bf:c8
5	192.168.0.6	GEARGUY-XP2	00:d0:59:d8:10:20

Figure 6-6

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

Viewing, Selecting, and Saving Logged Information

The 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: 2003-08-26 07:42:13

```
Tue, 2003-08-26 06:04:14 - Send out NTP request
Tue, 2003-08-26 06:04:14 - Receive NTP Reply
Tue, 2003-08-26 07:17:17 - Administrator login
Tue, 2003-08-26 07:26:19 - Administrator login
Tue, 2003-08-26 07:26:32 - Administrator login
Tue, 2003-08-26 07:29:48 - Administrator login
Tue, 2003-08-26 07:38:12 - TCP Packet - Source
Tue, 2003-08-26 07:38:39 - ICMP Packet - Source
Tue, 2003-08-26 07:38:42 - TCP Packet - Source
Tue, 2003-08-26 07:39:43 - TCP Packet - Source
Tue, 2003-08-26 07:39:49 - ICMP Packet - Source
Tue, 2003-08-26 07:39:49 - TCP Packet - Source
Tue, 2003-08-26 07:41:29 - TCP Packet - Source
```

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 6-7

Log entries are described in [Table 6-4](#) below:

Table 6-4. 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 6-5](#) below:

Table 6-5. 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 site
- Connections to the Web-based interface of the modem router
- Modem 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, 2002-05-21 18:48:39 - NETGEAR activated
```

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

```
Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2
```

```
Thu, 2002-05-21 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, 2002-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

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

```
wed, 2002-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was emailed.]

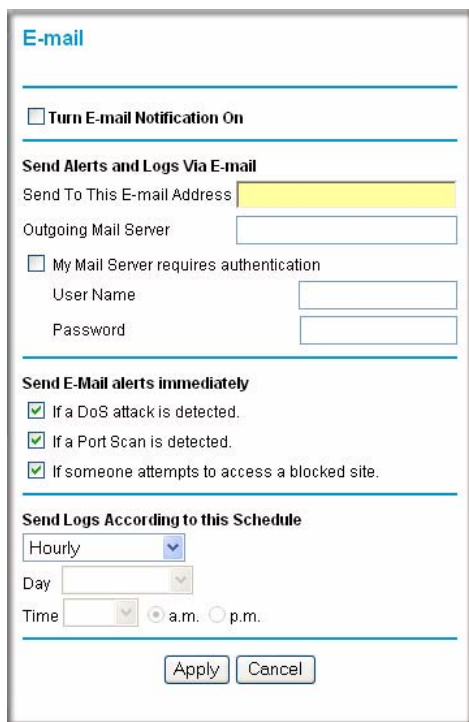
Dropped Packets

Wed, 2002-05-22 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, 2002-05-22 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, 2002-05-22 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:



The screenshot shows a web form titled "E-mail" with the following sections:

- Turn E-mail Notification On:** A checkbox that is currently unchecked.
- Send Alerts and Logs Via E-mail:**
 - Send To This E-mail Address: A text input field with a yellow background.
 - Outgoing Mail Server: A text input field.
 - My Mail Server requires authentication: An unchecked checkbox.
 - User Name: A text input field.
 - Password: A text input field.
- Send E-Mail alerts immediately:** Three checked checkboxes:
 - 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: A dropdown menu.
 - Day: A dropdown menu.
 - Time: A dropdown menu with radio buttons for "a.m." (selected) and "p.m.".

At the bottom of the form are "Apply" and "Cancel" buttons.

Figure 6-8

- **Turn e-mail notification on.** Select this check box if you want to receive e-mail logs and alerts from the modem router.
- **Send alerts and logs via email.**
 - **Send To This E-mail Address** Enter the e-mail address where you want to send the alerts and logs. Use a full e-mail address, such as ChrisXY@myISP.com.
 - **Outgoing Mail Server.** Enter the name or IP address of the outgoing SMTP mail server of your ISP (such as mail.myISP.com).
 - Check **My Mail Server requires authentication** if you need to login to your SMTP server to send E-mail. If you check this box, you must enter the user name and password for the mail server.



Tip: If you cannot remember the above information from when you set up your e-mail account, check the settings in your e-mail program.

- **Send alert 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.

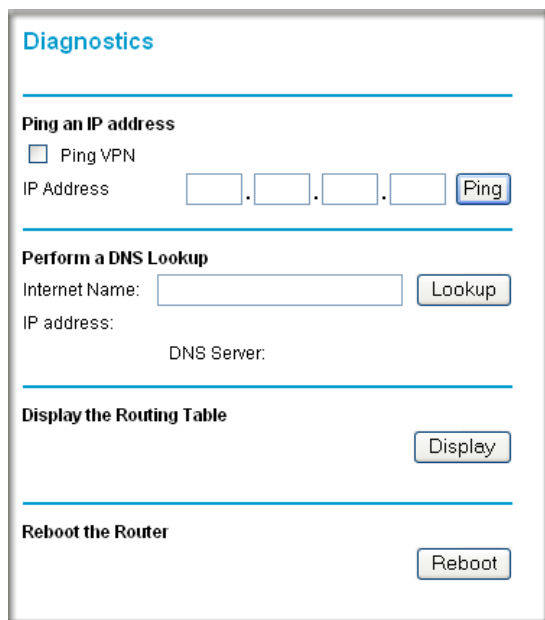
If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot e-mail the log file, the log buffer may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

Running Diagnostic Utilities and Rebooting the Modem Router

The ADSL Modem Wireless Router has a diagnostics feature. You can use the diagnostics menu to perform the following functions from the modem router:

- Ping an IP Address to test connectivity to see if you can reach a remote host. If Ping VPN is enabled, the ping packet always goes through the VPN if the VPN tunnel is enabled and working.
- Perform a DNS Lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing Table to identify what other modem routers the modem router is communicating with.
- Reboot the modem router to enable new network configurations to take effect or to clear problems with the modem router's network connection.

From the Main Menu of the browser interface, under the Maintenance heading, select the **Modem Router Diagnostics** heading to display the menu shown.



The screenshot shows the 'Diagnostics' menu with four sections:

- Ping an IP address**: Includes a checkbox for 'Ping VPN' and an 'IP Address' field with four input boxes and a 'Ping' button.
- Perform a DNS Lookup**: Includes an 'Internet Name' field, a 'Lookup' button, and 'IP address:' and 'DNS Server:' labels.
- Display the Routing Table**: Includes a 'Display' button.
- Reboot the Router**: Includes a 'Reboot' button.

Figure 6-9

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 54 Mbps ADSL Modem Wireless Router Model DG834G.



Tip: Be sure to change the 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 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 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:

Allow Remote Access By:

Only This Computer: [] . [] . [] . []

IP Address Range : From [] . [] . [] . []
To [] . [] . [] . []

Everyone

Port Number: [8080]

Apply Cancel

Figure 6-10

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

4. Specify what external addresses will be allowed to access the 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 modem router from the Internet, you will type your modem router's WAN IP address in your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter in your browser:

`http://134.177.0.123:8080`



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

Chapter 7

Advanced Configuration

This chapter describes how to configure the advanced features of your 54 Mbps ADSL Modem Wireless Router Model DG834G.

Configuring Advanced Security

The 54 Mbps ADSL Modem Wireless Router Model DG834G 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
- Wireless Bridging and Repeating

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 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.



Warning: 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 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 modem router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the modem router.

- From the Main Menu, under Advanced, click the **WAN Setup** link to view the page shown:

WAN Setup

Connect Automatically, as Required

Enable PPPoE-RELAY

Disable Port Scan and DOS Protection

Default DMZ Server 192 . 168 . 0 .

Respond to Ping on Internet WAN Port

MTU Size (in bytes) 1458

Figure 7-1

- Select the **Default DMZ Server** check box.
- Type the IP address for that server.
- 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.

Enable PPPoE-Relay

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

Disable Port Scan and DOS Protection

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

Respond to Ping on Internet WAN Port

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

- LAN IP 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


Add Edit Delete

Apply Cancel

Figure 7-2

The LAN TCP/IP Setup parameters are:

- **IP Address**
This is the LAN IP address of the modem router.

	<p>Warning: If you change the LAN IP address of the modem router while connected through the browser, you or anyone else using the router will be disconnected. You must then open a new connection to the new IP address and log in again. Others using the router will have to restart their computer and connect to the router again.</p>
---	---

- **IP Subnet Mask**
This is the LAN Subnet Mask of the modem router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router.

- **RIP Direction**

RIP (Router Information Protocol) allows a modem router to exchange routing information with other routers. The RIP Direction selection controls how the Modem Router sends and receives RIP packets. Both is the default.

- When set to Both or Out Only, the 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 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.

DHCP

By default, the 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 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 C](#) 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.

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

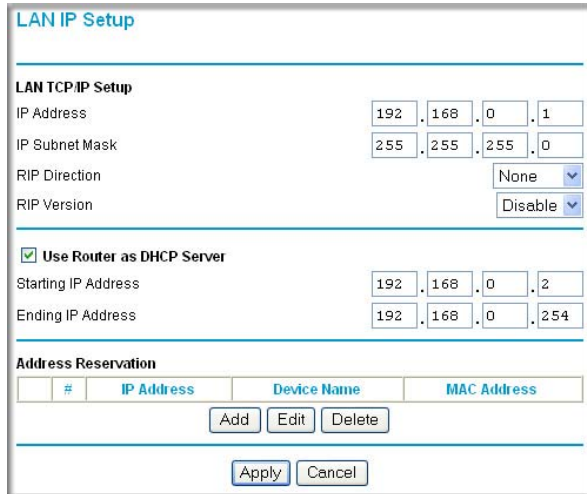
	<p>Note: The reserved address will not be assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.</p>
---	--

To edit or delete a reserved address entry:

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

How to Configure LAN TCP/IP Settings

- 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.
- From the Main Menu, under Advanced, click the **LAN IP Setup** link to view the menu, shown:



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 7-3

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