

Reference Manual for the Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV

NETGEAR

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

202-10169-01
September 2006

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Federal Communications Commission (FCC) Radiation Exposure Statement

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

European Union Statement of Compliance

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

Ěesky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erkläre NETGEAR, Inc., dass sich das Gerät Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
Français [French]	Par la présente NETGEAR, Inc. déclare que l'appareil Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarē, ka Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Lietuviø [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Direttiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oświadczam, że Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV jest zgodny z zasadniczymi wymogami oraz pozosta ^{ymi} stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV spáda základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 DG834GV product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV.

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: DG834GV
Publication Date: September 2006
Product Family: Modem Router
Product Name: Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV
Home or Business Product: Home
Language: English
Publication Part Number: 202-10169-01
Publication Version Number: 1.0

Contents

Reference Manual for the Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV

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
What's in the Box?	2-7
The Router's Front Panel	2-8
The Router's Rear Panel	2-9
Connecting the Router to the Internet	2-10

Chapter 3

Wireless Configuration

Considerations for a Wireless Network	3-1
Observe Performance, Placement, and Range Guidelines	3-1
Implement Appropriate Wireless Security	3-2
Understanding Wireless Settings	3-3
How to Set Up and Test Basic Wireless Connectivity	3-6

How to Restrict Wireless Access to Your Network	3-7
How to Configure WEP	3-10
How to Configure WPA-PSK	3-12
How to Configure WPA-802.1x	3-12

Chapter 4

VoIP and Telephone Settings

Configuring Advanced Security	4-1
Setting Up the Voice-over-IP Settings	4-2
Setting Up the PSTN Settings	4-3
Viewing the Voice Status	4-4
Viewing the Call Log	4-5

Chapter 5

Protecting Your Network

Protecting Access to Your Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV	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
Inbound Rules (Port Forwarding)	5-6
Outbound Rules (Service Blocking)	5-9
Order of Precedence for Rules	5-11
Services	5-12
How to Define Services	5-12
Setting Times and Scheduling Firewall Services	5-13
How to Set Your Time Zone	5-13
How to Schedule Firewall Services	5-15

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	6-3
How to Upgrade the Modem Router Firmware	6-3
Network Management Information	6-5
Viewing Modem Router Status and Usage Statistics	6-5
Viewing Attached Devices	6-10
Viewing, Selecting, and Saving Logged Information	6-10
Examples of Log Messages	6-13
Enabling Security Event E-mail Notification	6-14
Running Diagnostic Utilities and Rebooting the Modem Router	6-16
Enabling Remote Management	6-17
Configuring Remote Management	6-17

Chapter 7

Advanced Configuration

Configuring Advanced Security	7-1
Setting Up A Default DMZ Server	7-2
Connect Automatically, as Required	7-3
Disable Port Scan and DOS Protection	7-3
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	7-9
Configuring Dynamic DNS	7-10
How to Configure Dynamic DNS	7-10
Using Static Routes	7-12
Static Route Example	7-12
How to Configure Static Routes	7-13
Universal Plug and Play (UPnP)	7-14

Chapter 8

Troubleshooting

Basic Functioning	8-1
Power LED Not On	8-2
Test LED Never Turns On or Test LED Stays On	8-2
LAN or Internet Port LEDs Not On	8-3
Troubleshooting the Web Configuration Interface	8-3

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

Appendix A

Technical Specifications

Appendix B

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/DG834GV.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 Integrated ADSL Modem Wireless Router with Voice according to these specifications:

Table 1-2. Manual Scope

Product Version	Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV
Manual Publication Date	September 2006

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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV. The Integrated ADSL Modem Wireless Router with Voice 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 B](#) to become more familiar with the terms and procedures used in this manual.

About the Modem Router

The Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 Integrated ADSL Modem Wireless Router with Voice 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 Integrated ADSL Modem Wireless Router with Voice 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

These features are discussed below.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the DG834GV 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 DG834GV 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 Integrated ADSL Modem Wireless Router with Voice 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) encryption and 802.1x authentication
- Wireless access can be restricted by MAC address

Easy Installation and Management

You can install, configure, and operate the DG834GV 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 DG834GV 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 DG834GV supports Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). [“Internet Networking and TCP/IP Addressing” in Appendix B](#) provides further information on TCP/IP.

- The Ability to Enable or Disable IP Address Sharing by NAT
The DG834GV 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 DG834GV if you want to manage the IP address scheme yourself.
- Automatic Configuration of Attached PCs by DHCP
The DG834GV 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.

- **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 Integrated ADSL Modem Wireless Router with Voice 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 Integrated ADSL Modem Wireless Router with Voice 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 DG834GV 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 DG834GV 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.

What's in the Box?

The product package should contain the following items:

- Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV
- 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)
- *DG834GV Integrated ADSL Modem and Wireless Router Resource CD*, including this guide
- Two plastic feet that can be used to stand the Integrated ADSL Modem Wireless Router with Voice 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 Router's Front Panel

The front panel shown below contains status LEDs.

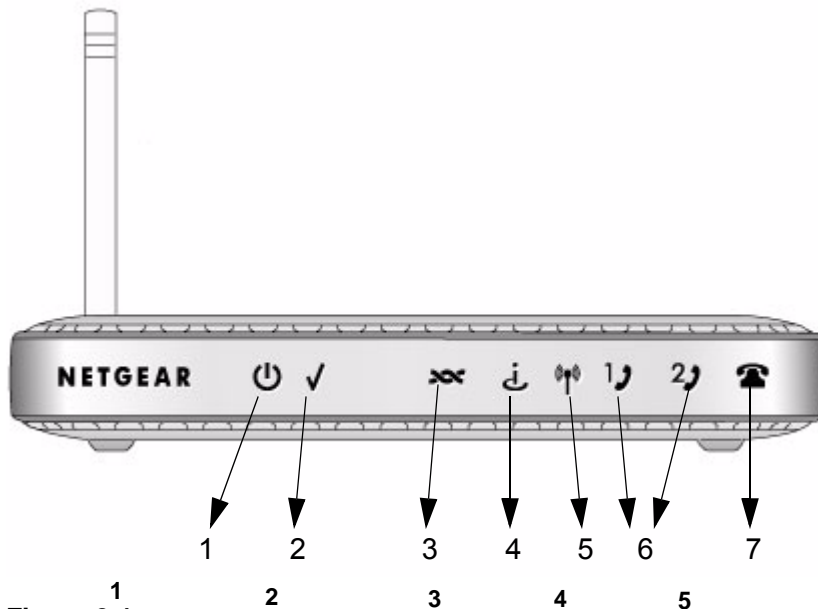


Figure 2-1

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

Table 2-1. LED Descriptions

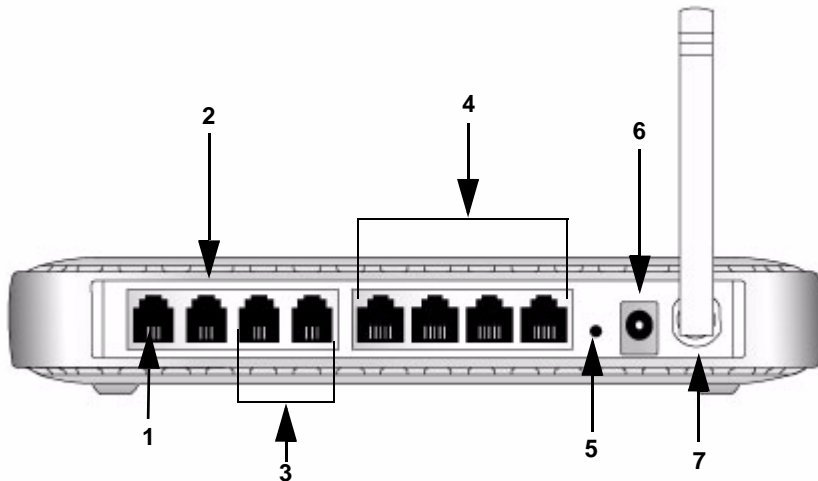
Label	Activity	Description
1. Power	On (Green) On (Red) Off	Power is supplied to the router. Power-on Self-test failure or device malfunction. Power is not supplied to the router.
2. Test	On (Amber) Blink (Amber) Off	System is not ready or failed to start up. The system is initializing. The system is ready and running.
3. ADSL	On (Green) Blink (Green) Off	ADSL is synchronized. DSL is attempting to synchronize. No link is detected on this port or modem is not powered on.

Table 2-1. LED Descriptions (continued)

4. Internet	On (Green) Flicker (Green) Red Off	Internet port is connected, has an IP address, DSL is up, no traffic detected. Traffic is passing through the connected internet port in either direction. Device attempted to connect, but failed. Modem powered off or in bridged mode, or ADSL connection not present.
5. Wireless	On (Green) Blink (Green) Off	Wireless port is linked. Data is being transmitted or received. No wireless link.
6. Phone1 Phone2	On (Green) Fast blink Slow blink Off	Registered to SIP server. Talking. Off hook. Phone not ready.
7. FXO/ PSTN fallback	On (Green) Blink Off	PSTN line detected. Talking. No PSTN line detected.

The Router's Rear Panel

The rear panel of the Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV (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-capable telephone wall jack via the ADSL port of an ADSL filter/splitter.
2. PSTN (Public Service Telephone Network) port for connecting to a telephone wall jack via the phone port of an ADSL filter/splitter.
3. Phone Ports for connecting to a telephones
4. Four Local Ethernet RJ-45 LAN ports for connecting the modem router to the local computers
5. Factory Default Reset push button
6. AC power adapter inlet
7. Wireless antenna

Each LAN port has two LEDs, one green and one amber. They indicate the port status as follows:

- On (Green) LAN port is linked to a 100Mbps device
- Blink (Green) Data is being transmitted or received at 100 Mbps
- On (Amber) LAN port is linked to a 10Mbps device
- Blink (Amber) Data is being transmitted or received at 10 Mbps
- Off No link is detected on this port

Connecting the Router to the Internet

To connect your Integrated ADSL Modem Wireless Router with Voice to the Internet, refer to the *Integrated ADSL Modem and Wirelesss Router Setup Manual* on the resource CD or online at <http://documentation.netgear.com/dg834gv/enu/208-10042-01/index.html>.

Chapter 3

Wireless Configuration

This chapter describes how to configure the wireless features of your Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV.

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 firewall. The latency, data throughput performance, and notebook power consumption also vary depending on your configuration choices.



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

For best results, place your firewall:

- Near the center of the area in which your computers will operate
- In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls)
- Away from sources of interference, such as computers, microwaves, and cordless phones
- 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 Integrated ADSL Modem Wireless Router with Voice provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

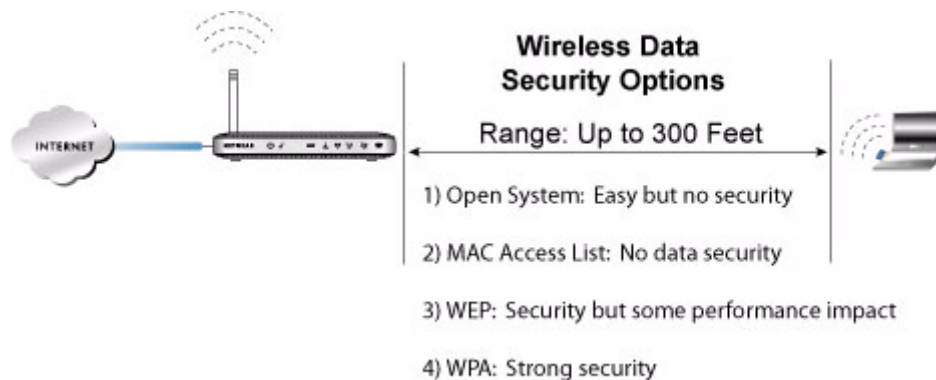


Figure 3-1

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

- **Restrict Access Based on MAC Address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the DG834GV. 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.
- **WPA.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame re-keying of WPA make it virtually impossible to compromise. Because this is a 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)


WPA-802.1x

Figure 3-2


The following parameters are in the Wireless Settings menu:

- **Wireless Network.**

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

	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 3-1. Wireless Security Options

Field	Description
Disable	Wireless security is not used.
WEP (Wired Equivalent Privacy)	<p>You can select the following WEP options:</p> <p>Authentication Type</p> <ul style="list-style-type: none"> • Open: the DG834GV does not perform any authentication. • Shared: WEP shared key authentication. For a full explanation of WEP shared key, see “Wireless Communications” in Appendix B. <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 DG834GV <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 DG834GV 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 3-1. Wireless Security Options (continued)

Field	Description
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	<p>WPA 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. For a full explanation of WPA, see “Wireless Communications” in Appendix B.</p> <p>Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.</p>
WPA-802.1x	<p>User authentication is implemented using 802.1x and RADIUS servers. For a full explanation of WPA, see “Wireless Communications” in Appendix B.</p> <p>Fill in the following:</p> <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 DG834GV 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 DG834GV 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 DG834GV 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 **Wireless**.



Note: The SSID of any wireless access adapters must match the SSID you configure in the Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV. If they do not match, you will not get a wireless connection to the DG834GV.

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

6. For initial configuration and test, leave the Wireless Card Access List set to allow everyone access by making sure that **Turn Access Control On** is *not* selected in the Wireless Station Access List. In addition, leave the Encryption Strength set to “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 firewall’s new settings.

8. Configure and test your computers for wireless connectivity.

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

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

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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV 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 3-3

Restricting Access to Your Network by Turning Off Wireless Connectivity

You can completely turn off the wireless portion of the DG834GV. 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 DG834GV 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 DG834GV. You must configure your wireless devices to match the wireless network name (SSID) you configure in the Integrated ADSL Modem Wireless Router with Voice.



Note: The SSID of any wireless access adapters must match the SSID you configure in the Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV. If they do not match, you will not get a wireless connection to the DG834GV.

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 DG834GV Integrated ADSL Modem Wireless Router with Voice 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
-------------	-------------

Add

Add New Station Manually

Device Name:

MAC Address:

Add

Apply Cancel

Figure 3-4

- 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 DG834GV. This prevents unauthorized access to your network.

How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the DG834GV firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the **Wireless Settings** link in the Setup section of the main menu for the DG834GV 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:

Figure 3-5

5. Select the **Authentication Type**.
6. Select the **Encryption Strength** setting.
7. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network.
- **Automatic** — enter a word or group of printable characters in the **Passphrase** box and click the **Generate** button. The four key boxes will be automatically populated with key values.
 - **Manual** — enter hexadecimal digits (any combination of 0-9, a-f, or A-F). Select which of the four keys will be active.
8. Select the radio button for the key you want to make active.
- Be sure you clearly understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one included in Windows XP only allow entry of one key which must match the default key you set in the DG834GV.
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



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, 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 DG834GV.
3. Choose the **WPA-PSK** radio button. The WPA-PSK page will display a WPA-PSK Security Encryption section.
4. Enter the pre-shared key in the Passphrase field.
5. Click **Apply** to save your settings.

How to Configure WPA-802.1x



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, 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 DG834GV.
3. Choose the **WPA-802.1x** radio button. The page will display the WPA-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 4

VoIP and Telephone Settings

This chapter describes how to configure the telephony features of your Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV.

Configuring the Telephony Settings

The Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV provides menus to configure and view the telephony settings. The settings are organized into two categories: VoIP (Voice over Internet Protocol) settings for internet telephony, and PSTN (Public Switched Telephone Network) settings for analog telephone fallback. The menus enable you to perform the following tasks:

- Configure the VoIP settings
- Configure the PSTN settings
- View the VoIP status
- View the call log

These features are discussed below.

Setting Up the Voice-over-IP Settings

Select **VoIP Settings** from the Telephony section of the main menu. The modem router will display a window similar to the following:

The screenshot shows the 'VoIP Settings' configuration window. It is organized into several sections:

- Service:** Includes checkboxes for 'TFTP Provisioning', 'Default Port' (set to 80), 'Primary Alternate Port' (set to 800), 'Secondary Alternate Port', and 'Configuration File'.
- SIP Proxy:** Includes 'SIP Proxy' (sipgate.de), 'SIP Control Port' (5060), 'SIP Local Port' (5060), 'Starting RTP Port' (10000), 'Use SIP Outbound Proxy' (unchecked), 'Outbound Proxy Address', and 'Outbound Proxy Port' (5060).
- VAD:** Includes 'VAD' (unchecked), 'Silence Detect Time' (0 msec), 'ATPM Action Key' (#), 'First-digit Timeout' (20 sec), and 'Last-digit Timeout' (5 sec).
- Line 1:** Includes 'Line Enable' (yes), 'Display Name' (5702004), 'Telephone Number' (5702004), 'User Name' (5702004), 'Password' (masked), 'Register Expire Time (sec)' (1200), 'Registration Head Start Time (sec)' (60), 'Distinctive Ring Valid' (unchecked), 'Prefer Ring ID' (0), 'Prefer Fax Codec' (Fax - G.711), and 'Prefer Codec' (G.711 u-Low @ 10ms). A 'Unregister' button is at the bottom.
- Line 2:** Includes 'Line Enable' (yes), 'Display Name' (5702006), 'Telephone Number' (5702006), 'User Name' (5702006), 'Password' (masked), 'Register Expire Time (sec)' (1200), 'Registration Head Start Time (sec)' (60), 'Distinctive Ring Valid' (unchecked), 'Prefer Ring ID' (0), 'Prefer Fax Codec' (Fax - G.711), and 'Prefer Codec' (G.711 u-Low @ 10ms). A 'Unregister' button is at the bottom.

At the bottom of the window are 'Apply' and 'Cancel' buttons.

Figure 4-1

The VoIP settings may be provisioned by your Voice Service Provider (VSP) in one of two different methods: TFTP provisioning or dialog-based provisioning. Refer to the instructions provided by your VSP, to ascertain which method to use.

If your VSP uses TFTP provisioning, set up your

If this modem router was provided by your VSP, the settings may be preconfigured. Otherwise, to set up your Voice account, refer to the instructions provided by your Voice Service Provider.

The Service section of the window is for setting up your SIP (Session Initiation Protocol) settings. SIP is a protocol for creating, modifying, and terminating telephony sessions over the internet.

Setting Up the PSTN Settings

Use the **PSTN Settings** menu to set which telephone numbers, if any, will be diverted to the PSTN line. You can specify a prefix that, when dialed before the telephone number, will cause the call to be diverted to the PSTN line. Also, specific numbers can always be diverted to the PSTN line.

1. Click the **PSTN Settings** link in the Telephony section of the main menu.

PSTN Settings

PSTN Relay
PSTN Prefix: *

PSTN Fixed Relay
Tel. No. 1:
Tel. No. 2:
Tel. No. 3:
Tel. No. 4:
These numbers are always sent via PSTN.

Emergency
Tel. No. 1:
Tel. No. 2:
Tel. No. 3:

Apply Cancel

Figure 4-2

2. To specify a prefix for diverting calls to the PSTN line, edit the entry in the **PSTN Prefix** text box. If you want to use only one character, it must be the * character. If you want to use more than one prefix character, the first character can be the * character or a digit, and all subsequent characters must be digits.

3. Add telephone numbers to the “PSTN Fixed Relay” and “Emergency” groups as required. Any numbers entered into either of these sections will always be diverted to the traditional analogue PSTN line without the need for dialing the PSTN prefix.
4. Click the **Apply** button to save your settings.

Viewing the Voice Status

The VoIP Status menu shows the current status of the Voice over IP connection. Click on the **VoIP Status** link in the Telephony section of the main menu.

The screenshot displays the 'VoIP Status' page with the following sections:

- Line 1**
 - Display Name
 - Telephone Number
 - Line 1 Status**
 - Hook State: ON
 - Registration State: Idle
 - Message Waiting: No
- Line 2**
 - Display Name
 - Telephone Number
 - Line 2 Status**
 - Hook State: ON
 - Registration State: Idle
 - Message Waiting: No
- Tftp Connection**
 - Last Attempt Time
 - Last Update Time
- Config File Information**
 - Default

A 'Refresh' button is located at the bottom of the page.

Figure 4-3

Line 1/Line 2

- **Display Name** is the name you chose when you first opened your account. Your display name will be visible to other individuals with caller ID.



Note: If your display name appears as "UNAVAILABLE", either your account has not been established or your router is unable to connect to the Internet.

- **Telephone Number** is the telephone number other people will use when they call you. This number was assigned to your router when you first established your account. Each line can have a different telephone number.



Note: If your Telephone Number appears as "phonenumber", either your account has not been established or your router has been unable to connect to the Internet.

Line 1/Line 2 Status

- **Hook State**—displays the condition of the telephone receiver. ON indicates the receiver is on its cradle, while OFF indicates the receiver is not seated on its cradle.
- **Registration State**—displays “Success” when your router has successfully connected to the VoIP servers. However, if you do not have a VOIP account or if the router could not connect to the VoIP servers, the status will be displayed as “Idle”.

Viewing the Call Log

Note to reviewers: All I got was one blank box with no buttons when this page was displayed. This was at odds with the information on the help page.

Chapter 5

Protecting Your Network

This chapter describes how to use the basic firewall features of the Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV to protect your network.

Protecting Access to Your Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV

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

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

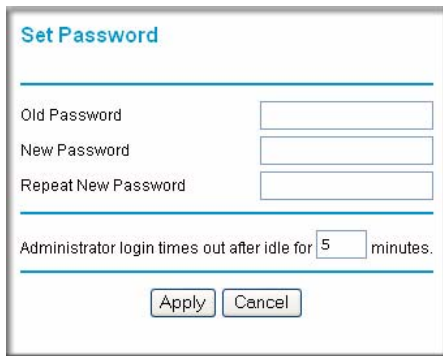



Figure 5-2

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

- In the Set Password menu, type a number in 'Administrator login times out' field. The suggested default value is 5 minutes.
- 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 Integrated ADSL Modem Wireless Router with Voice 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 Integrated ADSL Modem Wireless Router with Voice 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 in the **Content Filtering** section of the main 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 DG834GV 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 5-11](#) for more details.

To access the rules configuration of the DG834GV, 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

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**.

Inbound Rules (Port Forwarding)

Because the DG834GV 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.

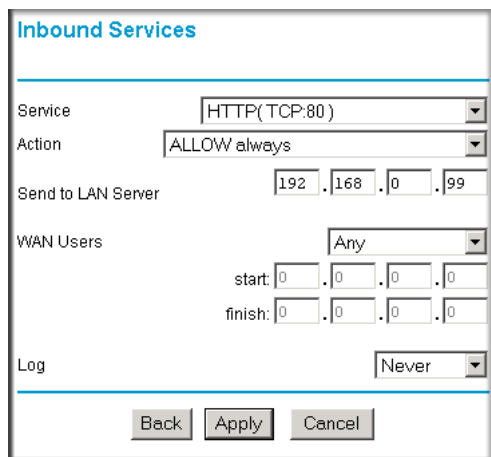


Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable 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 a configuration window titled "Inbound Services". It contains the following fields and controls:

- Service:** A dropdown menu with "HTTP(TCP:80)" selected.
- Action:** A dropdown menu with "ALLOW always" selected.
- Send to LAN Server:** IP address input fields showing "192", ".168", ".0", ".99".
- WAN Users:** A dropdown menu with "Any" selected.
- start:** IP address input fields showing "0", ".0", ".0", ".0".
- finish:** IP address input fields showing "0", ".0", ".0", ".0".
- Log:** A dropdown menu with "Never" selected.
- Buttons:** "Back", "Apply", and "Cancel" buttons at the bottom.

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 a configuration window titled "Inbound Services". It contains the following fields and values:

- Service: CU-SEEME(TCP/UDP:7648)
- Action: ALLOW always
- Send to LAN Server: 192 . 168 . 0 . 11
- WAN Users: Address Range
- start: 134 . 177 . 88 . 1
- finish: 134 . 177 . 88 . 254
- Log: Not Match

At the bottom of the window 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)

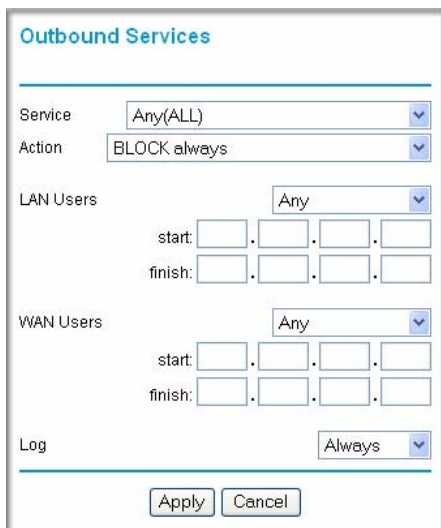
The DG834GV allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on:

- 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 'Any(ALL)' selected.
- Action:** A dropdown menu with 'BLOCK always' selected.
- LAN Users:** A dropdown menu with 'Any' selected. Below it are 'start:' and 'finish:' fields, each with four small input boxes for IP address digits.
- WAN Users:** A dropdown menu with 'Any' selected. Below it are 'start:' and 'finish:' fields, each with four small input boxes for IP address digits.
- Log:** A dropdown menu with 'Always' selected.

At the bottom of the window, there are two buttons: '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.
- **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 DG834GV 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.

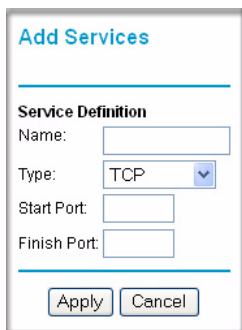
How to Define Services

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.



The screenshot shows a web form titled "Add Services". Under the heading "Service Definition", there are four input fields: "Name" (a text box), "Type" (a dropdown menu currently showing "TCP"), "Start Port" (a text box), and "Finish Port" (a text box). At the bottom of the form are two buttons: "Apply" and "Cancel".

Figure 5-10

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

Setting Times and Scheduling Firewall Services

The Integrated ADSL Modem Wireless Router with Voice 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 in the **Maintenance** section of the main menu, as shown below.

Schedule

Days:

Every Day
 Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Time of day: (use 24-hour clock)

All Day

Start Time Hour Minute
End Time Hour Minute

Time Zone

(GMT) Greenwich Mean Time : Edinburgh, London ▾

Adjust for Daylight Savings Time

Use this NTP Server . . .


Current Time: 2002-09-08 17:08:55

Apply Cancel

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.

	<p>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.</p>
---	--

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 in [Figure 5-11](#).
3. To block Internet services based on a schedule, select **Every Day** or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, enter Start Blocking and End Blocking times.
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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the Integrated ADSL Modem Wireless Router with Voice 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.

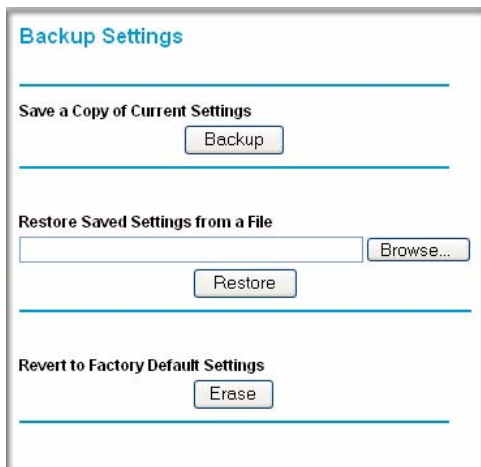


Figure 6-1

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 **Backup Settings** 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 Backup Settings 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 Router’s Rear Panel” on page 2-9](#).

Upgrading the Modem Router's Firmware

The software of the Integrated ADSL Modem Wireless Router with Voice 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.

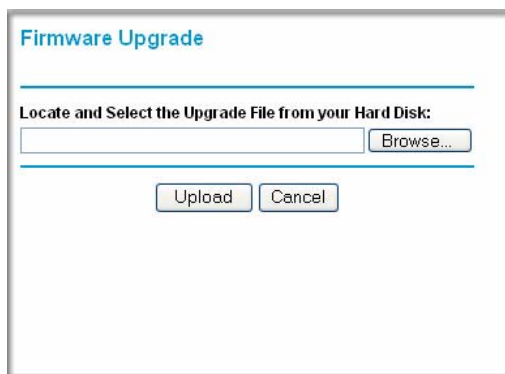


Figure 6-2

4. In the Modem Router Upgrade menu, click the **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 DG834GV 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 shows the 'Router Status' page with the following information:

Router Status	
Account Name	
Firmware Version	V0.01.26
ADSL Port	
MAC Address	00:0f:b5:d2:83:1d
IP Address	---
Network Type	PPPoE
IP Subnet Mask	---
Gateway IP Address	---
Domain Name Server	---
LAN Port	
MAC Address	00:0f:b5:d2:83:1c
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
Modem	
ADSL Firmware Version	5.00.02.00
Modem Status	Connecting
DownStream Connection Speed	0 kbps
UpStream Connection Speed	0 kbps
VPI	8
VCI	35
Wireless Port	
Name (SSID)	NETGEAR
Region	USA
Channel	11
Wireless AP	Enabled
Broadcast Name	Enabled

At the bottom of the page, there are two buttons: 'Show Statistics' and '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 3 for details.
Name (SSID)	The Service Set ID, also known as the wireless network name.
Region	The country where the unit is set up for use.
Channel	The current channel, which determines the operating frequency.
Wireless AP	Indicates if the Access Point feature is disabled or not. If not enabled, the Wireless LED on the front panel will be off.
Broadcast Name	Indicates if the DG834GV is configured to broadcast its SSID.

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

System Up Time 05:17:31							
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	4319	4826	0	46	24	05:17:26
WLAN	11M/54M	2272	46	0	10	0	05:17:19

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 parameters and three buttons at the bottom.

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". It contains a table with three columns: "IP Address", "Device Name", and "MAC Address". The table has one row of data. Below the table is a "Refresh" button.

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

Refresh

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 by clicking the **Logs** link in the **Content Filtering** section of the main menu.

An example of the logs file is shown below.

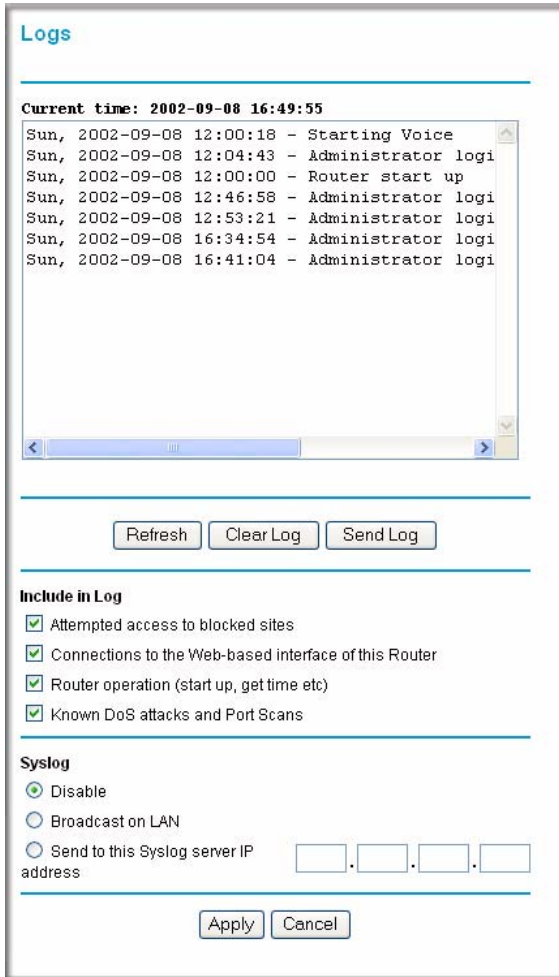


Figure 6-7

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-based configuration window titled "E-mail". It contains several sections for setting up email alerts:

- Turn E-mail Notification On:** A checkbox that is currently unchecked.
- Send Alerts and Logs Via E-mail:** A section with input fields for "Send To This E-mail Address", "Outgoing Mail Server", "User Name", and "Password". There is also a checkbox for "My Mail Server requires authentication".
- Send E-Mail alerts immediately:** A section with three checked checkboxes: "If a DoS attack is detected.", "If a Port Scan is detected.", and "If someone attempts to access a blocked site."
- Send Logs According to this Schedule:** A section with dropdown menus for "Hourly", "Day", and "Time", and radio buttons for "a.m." 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.

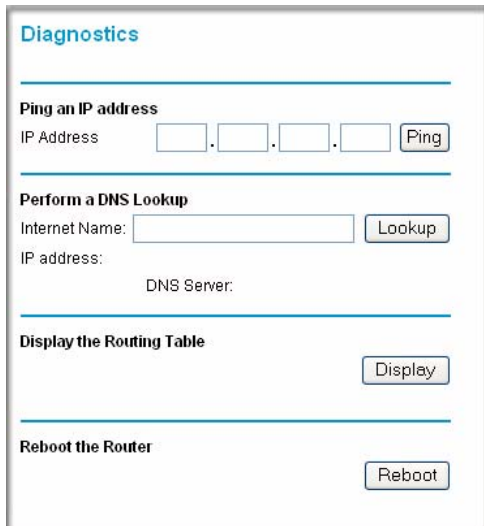
If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot e-mail the log file, the log buffer may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

Running Diagnostic Utilities and Rebooting the Modem Router

The Integrated ADSL Modem Wireless Router with Voice 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.
- 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 **Diagnostics** heading to display the menu shown.



The screenshot shows a web interface titled "Diagnostics" with a blue header. It contains four sections, each separated by a horizontal line:

- Ping an IP address:** A label "IP Address" followed by four input boxes for the IP address segments and a "Ping" button.
- Perform a DNS Lookup:** A label "Internet Name:" followed by an input box and a "Lookup" button. Below it, a label "IP address:" followed by an input box and a label "DNS Server:" followed by an input box.
- Display the Routing Table:** A "Display" button.
- Reboot the Router:** 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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV.



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 Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV.

Configuring Advanced Security

The Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV provides a variety of advanced features, such as:

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

These features are discussed below.

Setting Up A Default DMZ Server

The Default DMZ Server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The 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.

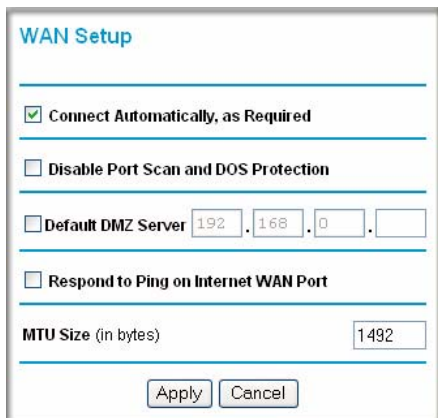
Incoming traffic from the Internet is normally discarded by the modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer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

Disable Port Scan and DOS Protection

Default DMZ Server 192 . 168 . 0 .

Respond to Ping on Internet WAN Port

MTU Size (in bytes) 1492

Apply Cancel

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.

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: RIP-1

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 B](#) for an explanation of DHCP and information about how to assign IP addresses for your network.

Use Router as DHCP server

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

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

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

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

Reserved IP addresses

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

To reserve an IP address:

1. Click the **Add** button.

Address Reservation

Address Reservation Table

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

IP Address: . . .

MAC Address:

Device Name:

Figure 7-3

2. In the IP Address box, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.
3. Type the MAC Address of the computer or server.



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

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



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

To edit or delete a reserved address entry:

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

How to Configure LAN TCP/IP Settings

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu, under Advanced, click the **LAN IP Setup** link to view the menu, shown:

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: RIP-1

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 7-4

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

Configuring Dynamic DNS

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

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

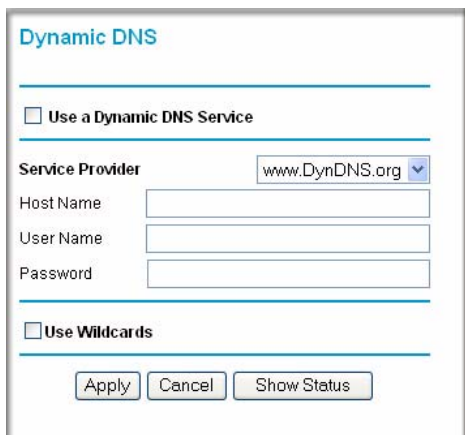
How to Configure Dynamic DNS



Warning: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the dynamic DNS service will not work because private addresses will not be routed on the Internet.

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

- From the Main Menu of the browser interface, under Advanced, select **Dynamic DNS** to display the page below.



Dynamic DNS

Use a Dynamic DNS Service

Service Provider:

Host Name:

User Name:

Password:

Use Wildcards

Apply Cancel Show Status

Figure 7-5

- Access the Web site of one of the dynamic DNS service providers whose names appear in the 'Service Provider' box, and register for an account.
For example, for dyndns.org, go to www.dyndns.org.
- Select the **Use a dynamic DNS service** check box.
- Select the name of your dynamic DNS Service Provider.
- Type the Host Name that your dynamic DNS service provider gave you.
The dynamic DNS service provider may call this the domain name. If your URL is `myName.dyndns.org`, then your Host Name is "myName."
- Type the User Name for your dynamic DNS account.
- Type the Password (or key) for your dynamic DNS account.
- If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature.
For example, the wildcard feature will cause `*.yourhost.dyndns.org` to be aliased to the same IP address as `yourhost.dyndns.org`
- Click **Apply** to save your configuration.

Using Static Routes

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

Static Route Example

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

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

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

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like [Figure 7-7](#).

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Modem Router IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- A Metric value of 1 will work since the ISDN router is on the LAN. This represents the number of routers between your network and the destination. This is a direct connection so it is set to 1.
- Private is selected only as a precautionary security measure in case RIP is activated.

How to Configure Static Routes

1. Log in to the router at its default LAN address of `http://192.168.0.1` with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, click **Static Routes** to view the Static Routes menu, shown in [Figure 7-6](#).

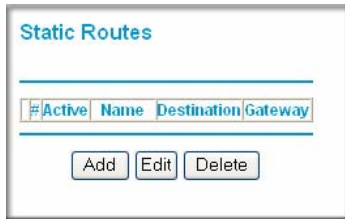


Figure 7-6

3. To add or edit a Static Route:
 - a. Click the **Edit** button to open the Edit Menu, shown in [Figure 7-7](#).

Static Routes

Route Name:

Private

Active

Destination IP Address: . . .

IP Subnet Mask: . . .

Gateway IP Address: . . .

Metric:

Buttons: Apply, Cancel

Figure 7-7

- b. Type a route name for this static route in the Route Name box under the table. This is for identification purpose only.
- c. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
- d. Select **Active** to make this route effective.

- e. Type the Destination IP Address of the final destination.
 - f. Type the IP Subnet Mask for this destination.
If the destination is a single host, type 255.255.255.255.
 - g. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.
 - h. Type a number between 1 and 15 as the Metric value.
This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
4. Click **Apply** to have the static route entered into the table.

Universal Plug and Play (UPnP)

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

1. Click **UPnP** on the main menu to invoke the UPnP menu:

UPnP

Turn UPnP On

Advertisement Period (in minutes)

Advertisement Time To Live (in hops)

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
YES	UDP	9212	20707	192.168.0.4
YES	TCP	10851	53226	192.168.0.4

Figure 7-8

2. Fill out the UPnP screen:
 - **Turn UPnP On:** UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the Router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the Router.

- **Advertisement Period:** The Advertisement Period is how often the Router will advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.
 - **Advertisement Time To Live:** The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.
 - **UPnP Portmap Table:** The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the Router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.
3. To save, cancel or refresh the table:
- a. Click **Apply** to save the new settings to the Router.
 - b. Click **Cancel** to disregard any unsaved changes.
 - c. Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Chapter 8

Troubleshooting

This chapter gives information about troubleshooting your Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?
- Have I connected the router correctly?
Go to [“Basic Functioning” on page 8-1.](#)
- I can’t access the router’s configuration with my browser.
Go to [“Troubleshooting the Web Configuration Interface” on page 8-3.](#)
- I’ve configured the router but I can’t access the Internet.
Go to [“Troubleshooting the ISP Connection” on page 8-4.](#)
- I can’t remember the router’s configuration password.
Go to [“Restoring the Default Configuration and Password” on page 8-9.](#)
- I want to clear the configuration and start over again.
Go to [“Restoring the Default Configuration and Password” on page 8-9.](#)

Basic Functioning

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

1. When power is first applied, verify that the Power LED is on (see [“The Router’s Front Panel” on page 2-8](#) for an illustration and explanation of the LEDs).
2. Verify that the Test LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 10 seconds, verify that:
 - a. The Test LED is not lit.

- b. The LAN port LEDs are lit for any local ports that are connected.
- c. The WAN port LED is lit.

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

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

Power LED Not On

If the Power and other LEDs are off when your router is turned on:

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

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

Test LED Never Turns On or Test LED Stays On

When the router is turned on, the Test LED turns on for about 10 seconds and then turns off. If the Test LED does not turn on, or if it stays on, there is a fault within the router.

If you experience problems with the Test LED:

- Cycle the power to see if the router recovers and the LED blinks for the correct amount of time.

If all LEDs including the Test LED are still on one minute after power up:

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in ["Using the Reset button" on page 8-9](#).

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

LAN or Internet Port LEDs Not On

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

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
 - When connecting the router's WAN ADSL port, use the cable that was supplied with the DG834GV.

Troubleshooting the Web Configuration Interface

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to [“Preparing a Computer for Network Access” in Appendix B](#) to find your computer's IP address.



Note: If your computer's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in [“Using the Reset button” on page 8-9](#).
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure the Java applet is loaded.

- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

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

Troubleshooting the ISP Connection

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

ADSL link

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

Internet LED Green or Blinking Green

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

Internet LED Blinking Amber

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

If the Internet LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

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

Internet LED Off

If the Internet LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

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

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

Obtaining a WAN IP Address

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

To check the WAN IP address from the browser interface:

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

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

- Your ISP may require a Multiplexing Method or Virtual Path Identifier/Virtual Channel Identifier parameter. Verify with your ISP the Multiplexing Method and parameter value, and update the router's ADSL Settings accordingly.

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

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

OR

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

Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

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

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



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

Troubleshooting Internet Browsing

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

- Your computer may not recognize any DNS server addresses.
A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the modem router's configuration, reboot your computer and verify the DNS address as described in [“Preparing a Computer for Network Access” in Appendix B](#). Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- Your computer may not have the modem router configured as its TCP/IP modem router.
If your computer obtains its information from the modem router by DHCP, reboot the computer and verify the modem router address as described in [“Preparing a Computer for Network Access” in Appendix B](#).

Troubleshooting a TCP/IP Network Using the Ping Utility

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

Testing the LAN Path to Your Router

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

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type Ping followed by the IP address of the router, as in this example:
`ping 192.168.0.1`
3. Click **OK**.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
 - Make sure the LAN port LED is on. If the LED is off, follow the instructions in [“LAN or Internet Port LEDs Not On”](#) on page 8-3.
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
 - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

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

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

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

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

- Check that your PC has the IP address of your router listed as the default modem router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default modem router as described in [“Preparing a Computer for Network Access”](#) in [Appendix B](#).
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to “clone” or “spoof” the MAC address from the authorized PC. Refer to your *Integrated ADSL Modem and Wireless Router Setup Manual*.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router’s administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the Web Configuration Manager (see [“Backing Up, Restoring, or Erasing Your Settings” on page 6-1](#)).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

Using the Reset button

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

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).
2. Release the Default Reset button and wait for the router to reboot.

Problems with Date and Time

The E-mail menu in the Content Filtering section displays the current date and time of day. The Integrated ADSL Modem Wireless Router with Voice uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

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

Appendix A

Technical Specifications

This appendix provides technical specifications for the Integrated ADSL Modem and Wireless Router with Voice, Model DG834GV.

Network Protocol and Standards Compatibility

Data and Routing Protocols: TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM

Power Adapter

North America: 120V, 60 Hz, input
United Kingdom, Australia: 240V, 50 Hz, input
Europe: 230V, 50 Hz, input
Japan: 100V, 50/60 Hz, input
All regions (output): 12 V AC @ 1.0A output

Physical Specifications

Dimensions: 6.9" x 4.7" x 1.1"
175 mm x 119 mm x 28 mm
Weight: 0.7 lbs.
0.3 kg

Environmental Specifications

Operating temperature: 0° to 40° C (32° to 104° F)
Operating humidity: 90% maximum relative humidity, noncondensing

Electromagnetic Emissions

Meets requirements of: FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B

Interface Specifications

LAN: 10BASE-T or 100BASE-Tx, RJ-45
WAN: ADSL, Dual RJ-11, pins 2 and 3, T1.413, G.DMT, G.Lite, ITU Annex A (for the DG834G) or ITU Annex B (for the DG834GB)

Appendix B

Related Documents

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

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

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>