

Reference Manual for the ADSL Modem Router DG834 v3

NETGEAR

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

202-10153-01
October 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 DG834 ADSL Modem Router je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr DG834 ADSL Modem Router overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklárt NETGEAR, Inc., dass sich das Gerát DG834 ADSL Modem Router in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme DG834 ADSL Modem Router vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this DG834 ADSL Modem Router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente NETGEAR, Inc. declara que el DG834 ADSL Modem Router cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR, Inc. ΔΗΛΩΝΕΙ ΟΤΙ DG834 ADSL Modem Router ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente NETGEAR, Inc. déclare que l'appareil DG834 ADSL Modem Router est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente NETGEAR, Inc. dichiara che questo DG834 ADSL Modem Router è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarā, ka DG834 ADSL Modem Router atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis DG834 ADSL Modem Router atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel DG834 ADSL Modem Router in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Malti [Maltese]	Hawnhekk, NETGEAR, Inc., jiddikjara li dan DG834 ADSL Modem Router jikkonforma mal-tijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a DG834 ADSL Modem Router megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oświadczam, że DG834 ADSL Modem Router jest zgodny z zasadniczymi wymogami oraz pozosta ³ ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este DG834 ADSL Modem Router está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta DG834 ADSL Modem Router v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že DG834 ADSL Modem Router spáda základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että DG834 ADSL Modem Router tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna [utrustningstyp] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the DG834 v3 product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das DG834 ADSL Modem Router gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the DG834 ADSL Modem Router has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

WProduct and Publication Details

Model Number: DG834 v3
Publication Date: October 2006
Product Family: Modem Router
Product Name: DG834 ADSL Modem Router
Home or Business Product: Home
Language: English
Publication Part Number: 202-10153-01

Change History

Version	Date Published	Change Description
1.0	January 2006	Original publication
1.1	October 2006	Removed NETBIOS feature.

Contents

Reference Manual for the ADSL Modem Router DG834 v3

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
Easy Installation and Management	2-3
Protocol Support	2-3
Virtual Private Networking (VPN)	2-5
Auto Sensing and Auto Uplink™ LAN Ethernet Connections	2-5
Content Filtering	2-5
Trend Micro Home Network Security	2-5
What's in the Box?	2-6
The Modem Router's Front Panel	2-7
The Router's Rear Panel	2-8
Connecting the Router to the Internet	2-9

Chapter 3

Protecting Your Network

Protecting Access to Your DG834 ADSL Modem Router	3-1
How to Change the Built-In Password	3-1
Changing the Administrator Login Timeout	3-2
Configuring Basic Firewall Services	3-3
Blocking Keywords, Sites, and Services	3-3
How to Block Keywords and Sites	3-3

Firewall Rules	3-5
Inbound Rules (Port Forwarding)	3-6
Outbound Rules (Service Blocking)	3-9
Order of Precedence for Rules	3-11
Services	3-12
How to Define Services	3-12
Setting Times and Scheduling Firewall Services	3-13
How to Set Your Time Zone	3-13
How to Schedule Firewall Services	3-15
Trend Micro Home Network Security	3-15
Security Service Settings	3-16
Parental Controls Settings	3-18

Chapter 4

Managing Your Network

Backing Up, Restoring, or Erasing Your Settings	4-1
How to Back Up the Configuration to a File	4-1
How to Restore the Configuration from a File	4-2
How to Erase the Configuration	4-2
Upgrading the Modem Router's Firmware	4-2
How to Upgrade the Modem Router Firmware	4-3
Network Management Information	4-4
Viewing Modem Router Status and Usage Statistics	4-4
Viewing Attached Devices	4-8
Viewing, Selecting, and Saving Logged Information	4-8
Examples of Log Messages	4-11
Enabling Security Event E-mail Notification	4-12
Running Diagnostic Utilities and Rebooting the Modem Router	4-13
Enabling Remote Management	4-14
Configuring Remote Management	4-15

Chapter 5

Advanced Configuration

Configuring Advanced Security	5-1
Setting Up A Default DMZ Server	5-2
Connect Automatically, as Required	5-3
Disable Port Scan and DOS Protection	5-3

Respond to Ping on Internet WAN Port	5-4
MTU Size	5-4
Configuring LAN IP Settings	5-4
DHCP	5-6
How to Configure LAN TCP/IP Settings	5-8
Configuring Dynamic DNS	5-8
How to Configure Dynamic DNS	5-9
Using Static Routes	5-10
Static Route Example	5-10
How to Configure Static Routes	5-11
Universal Plug and Play (UPnP)	5-13

Chapter 6

Virtual Private Networking (Advanced Feature)

Overview of VPN Configuration	6-1
Client-to-Gateway VPN Tunnels	6-2
Gateway-to-Gateway VPN Tunnels	6-2
Planning a VPN	6-3
VPN Tunnel Configuration	6-5
How to Set Up a Client-to-Gateway VPN Configuration	6-6
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834 v3	6-6
Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC	6-11
How to Set Up a Gateway-to-Gateway VPN Configuration	6-20
VPN Tunnel Control	6-27
Activating a VPN Tunnel	6-27
Verifying the Status of a VPN Tunnel	6-30
Deactivating a VPN Tunnel	6-32
Deleting a VPN Tunnel	6-34
How to Set Up VPN Tunnels in Special Circumstances	6-36
Using Auto Policy to Configure VPN Tunnels	6-36
Using Manual Policy to Configure VPN Tunnels	6-46

Chapter 7

Troubleshooting

Basic Functioning	7-1
Power LED Not On	7-2
Test LED Never Turns On or Test LED Stays On	7-2

LAN or Internet Port LEDs Not On	7-2
Troubleshooting the Web Configuration Interface	7-3
Troubleshooting the ISP Connection	7-4
ADSL link	7-4
Obtaining a WAN IP Address	7-5
Troubleshooting PPPoE or PPPoA	7-6
Troubleshooting Internet Browsing	7-7
Troubleshooting a TCP/IP Network Using the Ping Utility	7-7
Testing the LAN Path to Your Router	7-7
Testing the Path from Your Computer to a Remote Device	7-8
Restoring the Default Configuration and Password	7-9
Using the Reset button	7-9
Problems with Date and Time	7-10

Appendix A

Technical Specifications

Appendix B

NETGEAR VPN Configuration

DG834 v3 to FVL328	B-1
Configuration Profile	B-1
Step-By-Step Configuration	B-2
DG834 v3 with FQDN to FVL328	B-6
Configuration Profile	B-6
Step-By-Step Configuration	B-8
Configuration Summary (Telecommuter Example)	B-14
Setting Up the Client-to-Gateway VPN Configuration (Telecommuter Example)	B-15
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office	B-15
Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office	B-17
Monitoring the VPN Tunnel (Telecommuter Example)	B-27
Viewing the PC Client's Connection Monitor and Log Viewer	B-27
Viewing the VPN Router's VPN Status and Log Information	B-28

Appendix C

Related Documents

Chapter 1

About This Manual

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

Audience, Scope, Conventions, and Formats

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

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

<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:

This manual is written for the DG834 ADSL Modem Router according to these specifications:



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

Table 1-2. Manual Scope

Product Version	DG834 ADSL Modem Router
Manual Publication Date	October 2006

	Note: Product updates are available on the NETGEAR, Inc. Web site at http://kbserver.netgear.com .
-------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------

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.



Note: 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 *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.
- 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 DG834 ADSL Modem Router. The DG834 ADSL Modem Router is a combination of a built-in ADSL modem, modem router, 4-port switch, and firewall which enables your entire network to safely share an Internet connection that otherwise would be used by a single computer.



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

About the Modem Router

The DG834 ADSL Modem Router 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 DG834 ADSL Modem Router provides multiple Web content filtering options, plus e-mail alerts and logging. 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.

The DG834 v3 also supports Trend Micro Home Network Security, a bundle of services that includes router-based Parental Controls and network-wide protection from viruses, Trojans, spyware, spam, and other Internet threats.

Key Features

The DG834 ADSL Modem Router provides the following features:

- A built-in ADSL modem
- A powerful, true firewall
- 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
- Support for Trend Micro Home Network Security

These features are discussed below.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the DG834 v3 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 DG834 v3 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.

Easy Installation and Management

You can install, configure, and operate the DG834 v3 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**
A wizard built into 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 DG834 v3 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 DG834 v3 supports Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). [“Internet Networking and TCP/IP Addressing:” in Appendix C](#) provides further information on TCP/IP.

- **The Ability to Enable or Disable IP Address Sharing by NAT**
The DG834 v3 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 DG834 v3 if you want to manage the IP address scheme yourself.

- **Automatic Configuration of Attached PCs by DHCP**
The DG834 v3 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 DG834 ADSL Modem Router provides a secure encrypted connection between your local area network (LAN) and remote networks or clients. It includes the following VPN features:

- Supports 5 VPN connections.
- Supports industry standard VPN protocols
The DG834 ADSL Modem Router supports standard Manual or IKE keying methods, standard MD5 and SHA-1 authentication methods, and standard DES and 3DES encryption methods. It is compatible with many other VPN products.
- Supports 3DES encryption for maximum security.
- VPN Wizard based on VPNC recommended settings.

Auto Sensing and Auto Uplink™ LAN Ethernet Connections

With its internal 4-port 10/100 switch, the DG834 v3 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 DG834 v3 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.

Trend Micro Home Network Security

This service bundle from Trend Micro has three components:

- **Trend Micro dashboard**
This component is free for unlimited use. From the dashboard you can:
 - Scan your computer and entire network for security vulnerabilities
 - View individual computer and network-wide security reports

- Detect and remove spyware
- View attempts to access content restricted by Parental Controls
- Purchase subscriptions for Parental Controls and Trend Micro Internet Security
- **Trend Micro Internet Security**
You can install this program on up to 10 computers and try it free for 60 days. Its features include:
 - Real-time and scheduled scanning to remove viruses, Trojans, spyware, and other Internet threats
 - Personal firewall
 - Network intruder detection
 - Anti-spam
- **Router-based Parental Controls**
This service restricts home network users from viewing inappropriate Web content. It is free for 60 days, and when you register your free trial of Trend Micro Internet Security, your free use of Parental Controls is automatically extended to one year.

For instructions on activating these services, refer to [“Trend Micro Home Network Security” on page 3-15](#).

What’s in the Box?

The product package should contain the following items:

- DG834 ADSL Modem Router
- 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)
- *ADSL Modem Router Resource CD*, including this guide
- A Printed Quick Installation Guide
- Warranty and Support Information Cards
- Two plastic feet that can be used to stand the DG834 ADSL Modem Router on end.

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

The Modem Router's Front Panel

The DG834 ADSL Modem Router front panel shown below contains status LEDs.

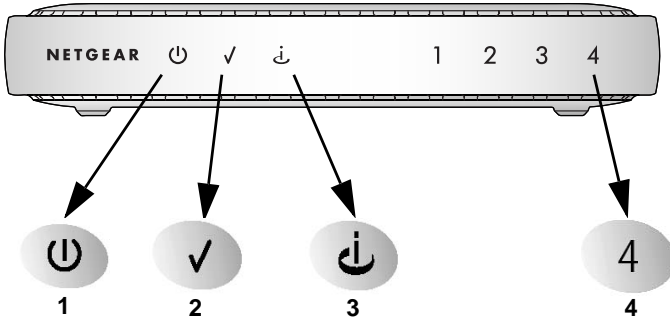


Figure 2-1

You can use the LEDs to verify various conditions. [Table 2-1](#) lists and describes each LED on the front panel of the modem router. These LEDs are green when lit.

Table 2-1. LED Descriptions

Label	Activity	Description
1. Power	On Off	Power is supplied to the modem router. Power is not supplied to the modem router.
2. Test	On Off	The system is initializing. The system is ready and running.
3. Internet	Blink — Amber On — Green Blink — Green	Indicates ADSL training. The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
4. LAN	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The Local port has detected a link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected a link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected on this port.

The Router's Rear Panel

The rear panel of the DG834 ADSL Modem Router ([Figure 2-2](#)) contains port connections.

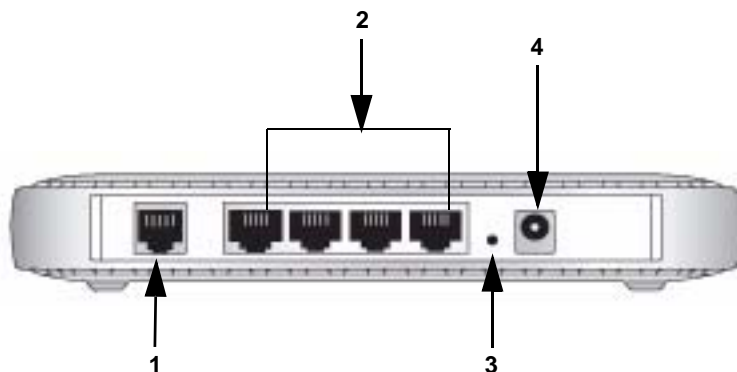


Figure 2-2

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

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

Connecting the Router to the Internet

To connect your DG834 ADSL Modem Router to the Internet, refer to the *ADSL Modem Router Setup Manual* on the *ADSL Modem Router Resource CD* or online as shown in the following table.

Table 2-1.

Language	URL
Dutch	http://documentation.netgear.com/dg834/nld/208-10032-01/
English	http://documentation.netgear.com/dg834/enu/208-10026-01/
French	http://documentation.netgear.com/dg834/fra/208-10027-01/
German	http://documentation.netgear.com/dg834/deu/208-10028-01/
Italian	http://documentation.netgear.com/dg834/ita/208-10029-01/
Spanish	http://documentation.netgear.com/dg834/esp/208-10030-01/
Swedish	http://documentation.netgear.com/dg834/sve/208-10031-01/

Chapter 3

Protecting Your Network

This chapter describes how to use the basic firewall features of the DG834 ADSL Modem Router to protect your network. It also describes how to configure Trend Micro Home Network Security.

Protecting Access to Your DG834 ADSL Modem Router

For security reasons, the modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login 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.

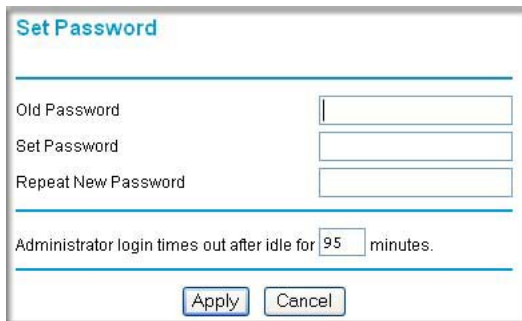
How to Change the Built-In Password

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 3-1

2. From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in [Figure 3-2](#).



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

Figure 3-2

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



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

Changing the Administrator Login Timeout

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

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

Configuring Basic Firewall Services

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

Blocking Keywords, Sites, and Services

The modem router provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the DG834 ADSL Modem Router prevents objectionable content from reaching your PCs. The modem router allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

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

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

How to Block Keywords and Sites

The DG834 ADSL Modem Router allows you to restrict access to Internet content based on functions such as Web addresses and Web address keywords.

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

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

Block Sites

Keyword Blocking

Never

Per Schedule

Always

Type Keyword or Domain Name Here.

Add Keyword

Block Sites Containing these Keywords or Domain Names:

Delete Keyword Clear List

Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address ...

Apply Cancel

Figure 3-3

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.



Note: The Block Sites feature is disabled when the Trend Micro Home Security feature is enabled. This is because the Trend security system has incorporates its own site-blocking capability.

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 DG834 v3 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 3-11](#) for more details.

To access the rules configuration of the DG834 v3, 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	Match

Add Edit Move Delete

Apply Cancel

Figure 3-4

- 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 DG834 v3 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.

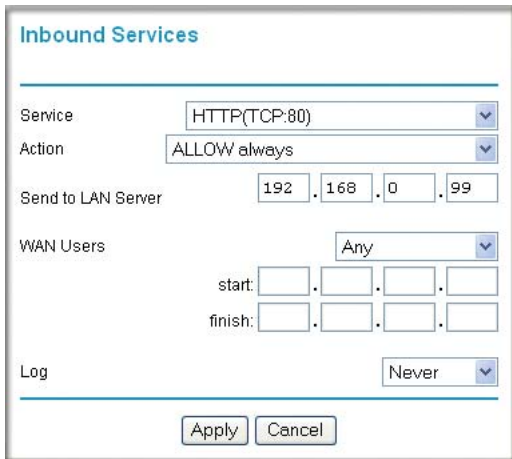


Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable 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 in [Figure 3-5](#):



The screenshot shows the 'Inbound Services' configuration window. It has a title bar 'Inbound Services' and a blue header. Below the header, there are several fields and dropdown menus: 'Service' is set to 'HTTP(TCP:80)', 'Action' is set to 'ALLOW always', 'Send to LAN Server' is set to '192.168.0.99', 'WAN Users' is set to 'Any', 'start:' and 'finish:' are empty, and 'Log' is set to 'Never'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Figure 3-5

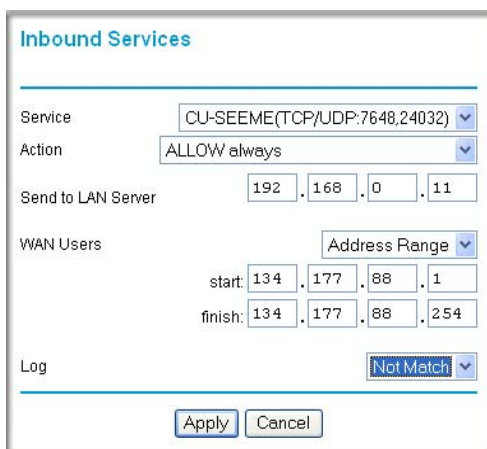
The parameters are:

- **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 in [Figure 3-6](#), CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.



The screenshot shows the 'Inbound Services' configuration window. The 'Service' dropdown is set to 'CU-SEEME(TCP/UDP:7648,24032)'. The 'Action' dropdown is set to 'ALLOW always'. The 'Send to LAN Server' field contains the IP address '192.168.0.11'. The 'WAN Users' dropdown is set to 'Address Range'. The 'start' field is set to '134.177.88.1' and the 'finish' field is set to '134.177.88.254'. The 'Log' dropdown is set to 'Not Match'. At the bottom, there are 'Apply' and 'Cancel' buttons.

Figure 3-6

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menu so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer's IP address constant.
- Local computers must access the local server using the computer's local LAN address (192.168.0.11 in the example in [Figure 3-6](#) above). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The DG834 v3 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'. Below the title bar, there are several fields and dropdown menus. The 'Service' dropdown is set to 'AIM(TCP:5190)'. The 'Action' dropdown is set to 'BLOCK by schedule, otherwise Allow'. There are two sections for IP address ranges: 'LAN Users' and 'WAN Users'. Each section has a dropdown menu set to 'Any' and two rows of input fields for 'start' and 'finish' IP addresses. At the bottom, there is a 'Log' dropdown set to 'Always' and two buttons: 'Apply' and 'Cancel'.

Figure 3-7

The parameters are:

- **Service**
From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Add Custom Service feature to add any additional services or applications that do not already appear.
- **Action**
Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **LAN Users**
These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:
 - Any — all IP addresses are covered by this rule.
 - Address range — if this option is selected, you must enter the Start and Finish fields.

- Single address — enter the required address in the Start field.
- WAN Users
These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the desired option:
 - Any — all IP addresses are covered by this rule.
 - Address range —if this option is selected, you must enter the Start and Finish fields.
 - Single address — enter the required address in the Start field.
- Log
You can select whether the traffic will be logged. The choices are:
 - Never — no log entries will be made for this service.
 - Always — any traffic for this service type will be logged.
 - Match — traffic of this type that matches the parameters and action will be logged.
 - Not match — traffic of this type that does not match the parameters and action will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in [Figure 3-8](#):

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 3-8

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 DG834 v3 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 in [Figure 3-9](#):



Figure 3-9

- To create a new Service, click the Add Custom Service button.

- To edit an existing Service, select its button on the left side of the table and click Edit Service.
 - To delete an existing Service, select its button on the left side of the table and click Delete Service.
3. Use the page shown below to define or edit a service.

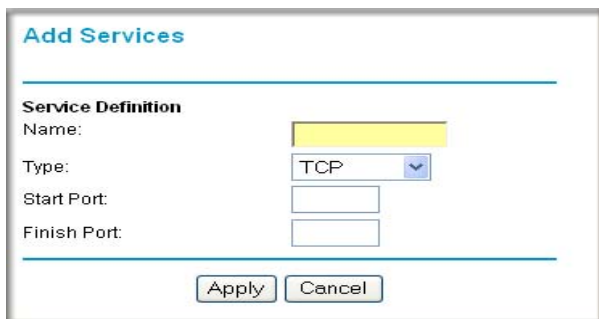


Figure 3-10

4. Click Apply to save your changes.

Setting Times and Scheduling Firewall Services

The DG834 ADSL Modem Router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet.

How to Set Your Time Zone

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

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

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

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: 2002-09-10 02:42:17

Apply Cancel

Figure 3-11

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 above in [Figure 3-11](#).
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.

Trend Micro Home Network Security

You can enable Home Network Security as described in this section if you did not do so when you originally set up your router. Home routers provide an enhanced Internet experience, but the likelihood of attacks also increases. Trend Micro Home Network Security addresses the security needs of computers accessing the Internet via home routers.



Note: The DG834 ADSL Modem Router supports Home Network Security. To take advantage of this feature you must register an account with Trend Micro. For more information, refer to the Home Network Security *Quick Start Guide* on the NETGEAR Resource CD, or to <http://www.trendmicro.com/offers/netgear>. The Trend Micro software requires Microsoft Internet Explorer 5.5 or higher.

To begin using Home Network Security, configure the Security Service and Parental Controls menus on your DG834 ADSL Modem Router. Each screen has a GUI button to click that will take you to the Trend Micro Web site to open your Trend Micro account.



Note: Because of overlapping functionality, the Block Sites feature, described in “[How to Block Keywords and Sites](#)” on page 3-3, is disabled if you enable Trend Micro Home Security.

Security Service Settings

Click Security Service under Content Filtering on the Main menu to get the Security Service Settings menu shown below:

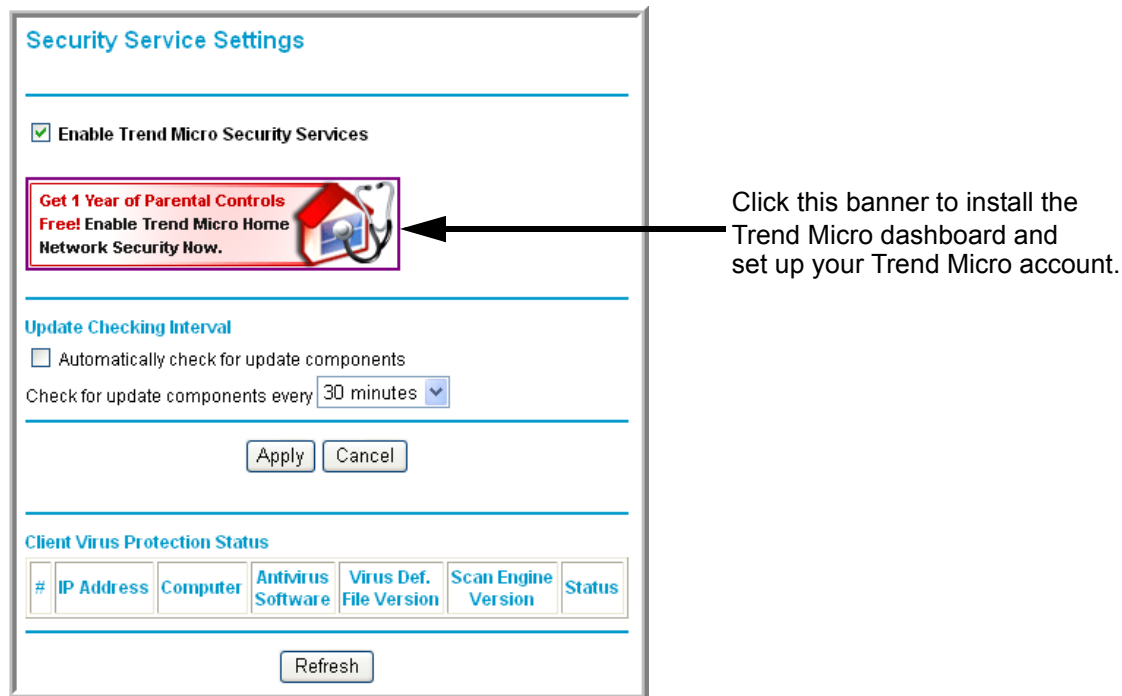


Figure 3-12

To install Home Network Security, click the Trend Micro banner and then follow the on-screen instructions. For assistance, refer to the Home Network Security *Quick Start Guide* included on the NETGEAR Resource CD. (You can download this document and the Home Network Security *User's Guide* at <http://www.trendmicro.com/en/support/tmss/netgear>.)

- **Enable Trend Micro Security Services.** Select this check box and then click Apply to enable the Security Service features on this page (automatic updates and Client Virus Protection Status information).
- **Automatically check for update components.** Select this check box to automatically check for updates to Trend Micro scanning components. Choose the desired checking interval from the list, and then click Apply.



Note: If your ISP bills by the amount of time or traffic you use, set the update frequency to once a day.

- **Client Virus Protection Status.** Provides information on all computers on your network.
 - **IP Address:** The computer's IP address
 - **Computer Name:** The name of the computer (as shown in Control Panel > System)
 - **Antivirus Software:** The type of antivirus software installed on the computer
 - **Virus Def. File Version:** The version of the virus pattern file in use by the antivirus software
 - **Scan Engine:** The version of the scan engine in use by the antivirus software
 - **Status:** Indicates if the virus pattern file or scan engine require updating (if no recognized antivirus software is found, the status is "Potential Threat")

Parental Controls Settings

Click Parental Controls under Content Filtering on the Main menu to get the Trend Micro Parental Controls menu shown below:

Click this banner to install the Trend Micro dashboard and set up your Trend Micro account.

Parental Controls Access Log

From: September 19, 2005

Category	Access Attempts	Times Accessed
Adult/Mature	0	0
Pornography	0	0
Sex Education	0	0
Intimate Apparel/Swimsuit	0	0
Nudity	0	0
Alcohol/Tobacco	0	0
Illegal/Questionable	0	0
Gambling	0	0
Violence/Hate/Racism	0	0
Weapons	0	0
Illegal Drugs	0	0
Hacking/Proxy Avoidance	0	0

Refresh Restart Log

Figure 3-13

To configure Parental Controls:

- Click Always to turn on Parental Controls all the time.
- Click Never to turn off Parental Controls.
- Click Per Schedule to turn on Parental Controls at the times specified on the Schedule page.



Note: After changing Parental Controls settings, click Apply to save changes.

To select Parental Controls Mode:

- Click Use General Controls to select General mode. In General mode, one access profile applies to all users.
- Click Use Per-User Controls to select Per-User mode. In Per-User mode, each user has an individual access profile.



Note: When in Per-User mode, everyone accessing the Internet through the router is required to log in.

To configure General mode:

1. Enter a password in the Parental Controls Bypass Password box, re-enter it in the Confirm password box, and then click Apply. This password allows users to access pages that are blocked by Parental Controls.
2. Select the access profile that will apply to all users, as follows:
 - a. To select a predefined profile, click Apply Profile and then choose a profile from the list.
 - b. To create a custom profile, click Use Custom Settings and then select the check boxes as desired. (For additional choices, click More Categories).
 - c. To allow unrestricted Internet access, click No Restrictions.
3. Click Apply.

To configure Per-User mode:

The User Account Information table in Per-User mode shows each user's name, access profile, and status. Users with Active status can access the Internet sites permitted by their access profiles. Users with Inactive status cannot log in and cannot access any Internet sites.

To add a new user:

1. Click Add. Type the new user's login name and password, and then re-enter the password in the Confirm password box.
2. Select the new user's status. To allow Internet access, click Active. To completely disable this user's Internet access, click Inactive.
3. Select the access profile that will apply to this user, as follows:
 - a. To select a predefined profile, click Apply Profile and then choose a profile from the list.

- b. To create a custom profile, click Use Custom Settings and then select the check boxes as desired. (For additional choices, click More Categories).
- c. To allow unrestricted Internet access, click No Restrictions.
- d. Click Apply.

To change a user's account information:

1. Select the user's name in the User Account Information table and then click Edit.
2. Make the desired changes, and then click Apply.

To delete a user, select the user's name in the User Account Information table and then click Delete.

Parental Controls Logs

Click Parental Controls Logs to view attempts to access restricted sites, and actual accesses.

Blocking criteria for potentially offensive categories

Trend Micro has defined twelve potentially offensive categories of Web sites. Following are the blocking criteria for each category:

- **Adult/Mature Content:** Sites that contain material of an adult nature but without excessive violence, sexual content, or nudity. These sites may include profane or vulgar content not appropriate for children.
- **Alcohol/Tobacco:** Sites that promote or sell alcohol and tobacco products. Includes sites that glamorize or otherwise encourage alcohol or tobacco use. Does not include sites that sell alcohol or tobacco as a subset of another business.
- **Gambling:** Sites where users can place bets or participate in betting pools (including lotteries) online. Also includes sites that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. Does not include sites that sell gambling-related products or machines. Also does not include offline casino and hotel sites, unless meeting one of the foregoing criteria).
- **Hacking/Proxy Avoidance:** Sites providing information on illegal or questionable access to, or use of, communications equipment and software, or that provide information on how to bypass proxy server features or gain unauthorized access to URLs.
- **Illegal Drugs:** Sites that promote, offer, sell, supply, or advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants and chemicals, and related paraphernalia.

- **Illegal/Questionable:** Sites that advocate or advise on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques, and plagiarism. Also includes sites that provide or sell questionable educational materials, such as term papers.
- **Intimate Apparel/Swimsuit:** Sites that contain images of swimsuits, intimate apparel, or other suggestive clothing. Does not include sites selling undergarments as a subset of another business.
- **Nudity:** Sites containing nude or seminude depictions of the human body. Such depictions need not be sexual in intent or effect. May include sites containing nude paintings or photo galleries of an artistic nature. This category includes nudist or naturist sites.
- **Pornography:** Sites that contain sexually explicit material.
- **Sex Education:** Sites that provide information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. Also includes sites that offer tips for better sex as well as products used for sexual enhancement.
- **Violence/Hate/Racism:** Sites depicting or advocating physical harm to people or property. Includes sites that convey hostility or aggression toward, or the denigration of, an individual or group on the basis of race, religion, gender, nationality, ethnic origin, and so forth.
- **Weapons:** Sites that sell, review, or describe guns, knives, martial arts devices, and related accessories. Does not include sites that promote weapons collecting, or groups that either support or oppose weapons ownership.

Chapter 4

Managing Your Network

This chapter describes how to perform network management tasks with your DG834 ADSL Modem Router.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the DG834 ADSL Modem Router are stored in a configuration file in the modem router. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.

How to Back Up the Configuration to a File

1. Log in to the modem router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the modem router.
2. From the Maintenance heading of the Main Menu, select the Backup Settings menu as seen in [Figure 4-1](#).

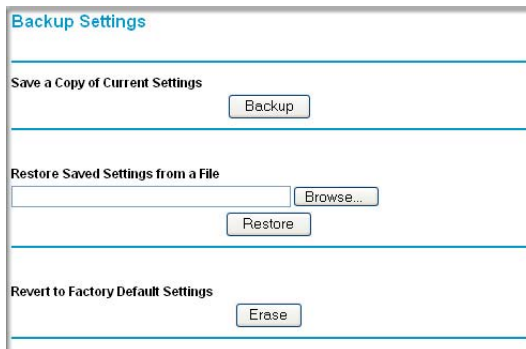


Figure 4-1

3. Click Backup to save a copy of the current settings.
4. Store the `.cfg` file on a computer on your network.

How to Restore the Configuration from a File

1. Log in to the modem router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the modem router.
2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in [Figure 4-1](#).
3. Enter the full path to the file on your network or click the Browse button to locate the file.
4. When you have located the `.cfg` file, click the Restore button to upload the file to the modem router.
5. The modem router will then reboot automatically.

How to Erase the Configuration

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

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

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



Note: To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the modem router. See [Figure 2-2 on page 2-8](#).

Upgrading the Modem Router's Firmware

The software of the DG834 ADSL Modem Router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

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

How to Upgrade the Modem Router Firmware



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

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

The Web browser used to upload new firmware into the 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 **Modem Router Upgrade** heading to display the menu shown in [Figure 4-2](#).

Figure 4-2

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



Note: When uploading software to the 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 DG834 v3 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, select Modem Router Status to view the screen in [Figure 4-3](#).

Router Status

<hr/>	
Account Name	
Firmware Version	0.01.14
<hr/>	
ADSL Port	
MAC Address	00:09:5b:70:46:26
IP Address	63.199.31.112
Network Type	PPPOE
IP Subnet Mask	255.255.255.255
Domain Name Server	206.13.31.12
<hr/>	
LAN Port	
MAC Address	00:09:5b:70:46:26
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
<hr/>	
Modem	
ADSL Firmware Version	1.00.05.00
Modem Status	Connected
DownStream Connection Speed	1536 kbps
UpStream Connection Speed	160 kbps
VPI	0
VCI	35
<hr/>	
<input type="button" value="Show Statistics"/> <input type="button" value="Connection Status"/>	

Figure 4-3

The Modem Router Status menu provides status and usage information.

This screen shows the following parameters:

Table 4-1. 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	Displays the modem router firmware version.
ADSL Port	These parameters apply to the Internet (ADSL) port of the modem router.
MAC Address	Displays the Ethernet MAC address being used by the Internet (ADSL) port of the modem router.
IP Address	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 on your ISP.
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)	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	Displays the Ethernet MAC address being used by the Local (LAN) port of the modem router.
IP Address	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	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.
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.

Click the Show Statistics button to display modem router usage statistics, as shown in [Figure 4-3](#) below:

System Up Time 16:54:13							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoE	1272	1642	0	12	81	04:26:50
LAN	10M/100M	24630	18474	0	72	24	16:54:11

ADSL Link	Downstream	Upstream
Connection Speed	3008 kbps	512 kbps
Line Attenuation	50.0 db	28.5 db
Noise Margin	9.2 db	20.0 db

Poll Interval : (secs)

Figure 4-4

This screen shows the following statistics:

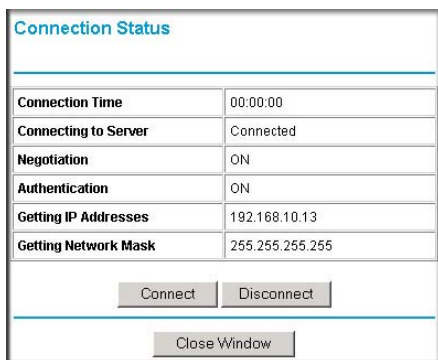
Table 4-1. Router Statistics Fields

Field	Description
WAN, LAN, or Serial Port	The statistics for the WAN (Internet), LAN (local), and Serial ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
Rx B/s	The average line utilization for this port.
Up Time	The time elapsed since the last power cycle or reset.
ADSL Link Downstream or Upstream	The statistics for the upstream and downstream ADSL link. These statistics will be of interest to your technical support representative if you are having problems obtaining or maintaining a connection.
Connection Speed	Typically, the downstream speed is faster than the upstream speed.

Table 4-1. Router Statistics Fields (continued)

Field	Description
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, as shown in [Figure 4-5](#) below:

**Figure 4-5**

Clicking the Renew button updates the status information.

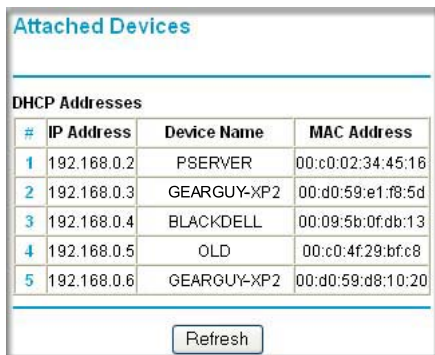
This screen shows the following statistics:

Table 4-1. 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 in [Figure 4-6](#):



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

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

Figure 4-6

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

Viewing, Selecting, and Saving Logged Information

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

An example of the logs file is shown below.

Logs

Current time: 2003-08-26 07:42:13

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

Refresh Clear Log Send Log

Include in Log

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

Syslog

- Disable
- Broadcast on LAN
- Send to this Syslog server IP address . . .

Apply Cancel

Figure 4-7

Log entries are described in [Table 4-1](#) below:

Table 4-1. 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 4-2](#) below:

Table 4-2. 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 page titled "E-mail". At the top, there is a section "E-mail" with a blue header. Below it, there is a checkbox labeled "Turn E-mail Notification On". Underneath, there is a section "Send Alerts and Logs Via E-mail" with a text input field for "Send To This E-mail Address" (highlighted in yellow), a text input field for "Outgoing Mail Server", and a checkbox for "My Mail Server requires authentication". Below this are two text input fields for "User Name" and "Password". The next section is "Send E-Mail alerts immediately" 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.". The final section is "Send Logs According to this Schedule" with a dropdown menu set to "Hourly", a "Day" dropdown menu, and a "Time" dropdown menu with radio buttons for "a.m." and "p.m.". At the bottom, there are "Apply" and "Cancel" buttons.

Figure 4-8

- **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.

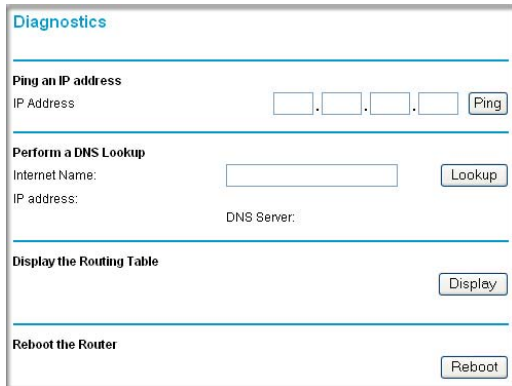
Running Diagnostic Utilities and Rebooting the Modem Router

The DG834 ADSL Modem Router has a diagnostics feature. You can use the diagnostics menu to perform the following functions from the modem router:

- Ping an IP Address to test connectivity to see if you can reach a remote host.
- Perform a DNS Lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing Table to identify what other modem routers the modem router is communicating with.

- Reboot the modem router to enable new network configurations to take effect or to clear problems with the modem router's network connection.

From the Main Menu of the browser interface, under the Maintenance heading, select the Modem Router Diagnostics heading to display the menu shown in [Figure 4-9](#).



The screenshot shows a web interface titled "Diagnostics". It contains four sections, each with a button:

- Ping an IP address:** A form with four input boxes for IP address digits and a "Ping" button.
- Perform a DNS Lookup:** A form with an "Internet Name:" input box and a "Lookup" button. Below it, there are labels for "IP address:" and "DNS Server:".
- Display the Routing Table:** A "Display" button.
- Reboot the Router:** A "Reboot" button.

Figure 4-9

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 DG834 ADSL Modem Router.



Note: 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.

Figure 4-10

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 5

Advanced Configuration

This chapter describes how to configure the advanced features of your DG834 ADSL Modem Router.

Configuring Advanced Security

The DG834 ADSL Modem Router provides a variety of advanced features, such as:

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

These features are discussed below.

Setting Up A Default DMZ Server

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



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

Incoming traffic from the Internet is normally discarded by the 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 in [Figure 5-1](#):

The screenshot shows the WAN Setup configuration interface. It includes the following elements:

- WAN Setup** (Section Header)
- Connect Automatically, as Required**
- Disable Port Scan and DOS Protection**
- Default DMZ Server** (with IP address fields: 192, 168, 0, .)
- Respond to Ping on Internet WAN Port**
- MTU Size (in bytes)** (with a text box containing 1492)
- Apply** and **Cancel** buttons at the bottom.

Figure 5-1

- 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: Disable

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

Add Edit Delete

Apply Cancel

Figure 5-2

The LAN TCP/IP Setup parameters are:

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



Note: If you change the LAN IP address of the modem router while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

DHCP

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

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See [“Internet Networking and TCP/IP Addressing:” in Appendix C](#) for an explanation of DHCP and information about how to assign IP addresses for your network.

Use Router as DHCP server

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

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

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

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

Reserved IP addresses

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

To reserve an IP address:

1. Click the **Add** button.
2. In the IP Address box, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.
3. Type the MAC Address of the computer or server.
Tip: If the computer is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.
4. Click **Apply** to enter the reserved address into the table.

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

To edit or delete a reserved address entry:

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

How to Configure LAN TCP/IP Settings

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu, under Advanced, click the LAN IP Setup link to view the menu, shown in [Figure 5-3](#):

LAN IP Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: Disable

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

Add Edit Delete

Apply Cancel

Figure 5-3

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

Configuring Dynamic DNS

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

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

How to Configure Dynamic DNS

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, select Dynamic DNS to display the page below.

Figure 5-4

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

9. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the Use wildcards check box to activate this feature.
For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
10. Click Apply to save your configuration.



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

Using Static Routes

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

Static Route Example

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

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

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the 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.

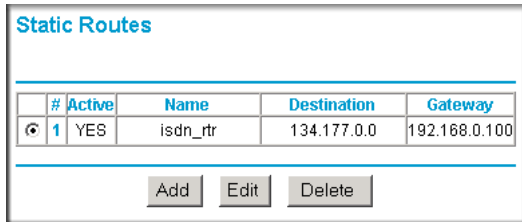
In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like [Figure 5-6](#).

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The 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 5-5](#).



#	Active	Name	Destination	Gateway
1	YES	isdn_rtr	134.177.0.0	192.168.0.100

Figure 5-5

3. To add or edit a Static Route:
 - a. Click the **Add** to add a new route or the **Edit** button to edit an existing route. The Static Routes screen will be displayed, as shown in [Figure 5-6](#).

Static Routes

Route Name

Private

Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

Figure 5-6

- b. Type a route name for this static route in the Route Name box under the table. This is for identification purpose only.
 - c. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
 - d. Select **Active** to make this route effective.
 - e. Type the Destination IP Address of the final destination.
 - f. Type the IP Subnet Mask for this destination. If the destination is a single host, type 255.255.255.255.
 - g. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.
 - h. Type a number between 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:

Figure 5-7

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 6

Virtual Private Networking (Advanced Feature)

This chapter describes how to use the virtual private networking (VPN) features of the DG834 ADSL Modem Router. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

This chapter is organized as follows:

- [“Overview of VPN Configuration” on page 6-1](#) provides an overview of the two most common VPN configurations: Client-to-Gateway and Gateway-to-Gateway.
- [“Planning a VPN” on page 6-3](#) provides a worksheet for recording the configuration parameters of the VPN you want to set up, along with the VPN Committee (VPNC) recommended default parameters set by the VPN Wizard.
- [“VPN Tunnel Configuration” on page 6-5](#) summarizes the three ways to configure a VPN tunnel: VPN Wizard (recommended for most situations), Auto Policy, and Manual Policy.
- [“How to Set Up a Client-to-Gateway VPN Configuration” on page 6-6](#) provides the steps needed to configure a VPN tunnel between a remote PC and a network gateway using the VPN Wizard and the NETGEAR ProSafe VPN Client.
- [“How to Set Up a Gateway-to-Gateway VPN Configuration” on page 6-20](#) provides the steps needed to configure a VPN tunnel between two network gateways using the VPN Wizard.
- [“VPN Tunnel Control” on page 6-27](#) provides the step-by-step procedures for activating, verifying, deactivating, and deleting a VPN tunnel once the VPN tunnel has been configured.
- [“How to Set Up VPN Tunnels in Special Circumstances” on page 6-36](#) provides the steps needed to configure VPN tunnels when there are special circumstances and the VPNC recommended defaults of the VPN Wizard are inappropriate. The two alternatives for configuring VPN tunnels are Auto Policy and Manual Policy.

Overview of VPN Configuration

Two common scenarios for configuring VPN tunnels are between a remote personal computer and a network gateway and between two or more network gateways. The DG834 v3 supports both of these types of VPN configurations. The DG834 ADSL Modem Router supports up to five concurrent tunnels.

Client-to-Gateway VPN Tunnels

Client-to-Gateway VPN Tunnels provide secure access from a remote PC, such as a telecommuter connecting to an office network (see [Figure 6-1](#)).

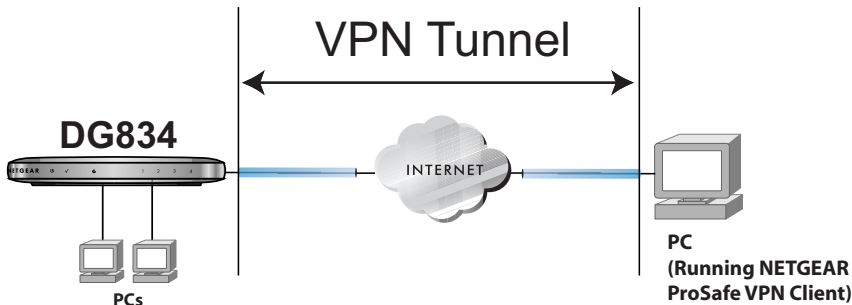


Figure 6-1

A VPN client access allows a remote PC to connect to your network from any location on the Internet. In this case, the remote PC is one tunnel endpoint, running the VPN client software. The DG834 ADSL Modem Router on your network is the other tunnel endpoint. See [“How to Set Up a Client-to-Gateway VPN Configuration”](#) on page 6-6 to set up this configuration.

Gateway-to-Gateway VPN Tunnels

- Gateway-to-Gateway VPN Tunnels provide secure access between networks, such as a branch or home office and a main office (see [Figure 6-2](#)).

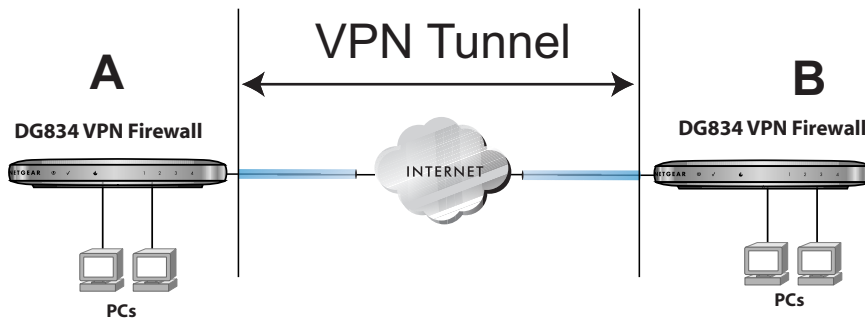


Figure 6-2

A VPN between two or more NETGEAR VPN-enabled routers is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use DG834 v3s on each end of the tunnel to form the VPN tunnel end points. See [“How to Set Up a Gateway-to-Gateway VPN Configuration”](#) on [page 6-20](#) to set up this configuration.

Planning a VPN

When you set up a VPN, it is helpful to plan the network configuration and record the configuration parameters on a worksheet:

Table 6-1. VPN Tunnel Configuration Worksheet

Connection Name:					_____
Pre-Shared Key:					_____
Secure Association -- Main Mode or Manual Keys:					_____
Perfect Forward Secrecy -- Enabled or Disabled:					_____
Encryption Protocol -- DES or 3DES:					_____
Authentication Protocol -- MD5 or SHA-1:					_____
Diffie-Hellman (DH) Group -- Group 1 or Group 2:					_____
Key Life in seconds:					_____
IKE Life Time in seconds:					_____
VPN Endpoint	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)	
_____	_____	_____	_____	_____	
_____	_____	_____	_____	_____	

To set up a VPN connection, you must configure each endpoint with specific identification and connection information describing the other endpoint. You must configure the outbound VPN settings on one end to match the inbound VPN settings on other end, and vice versa.

This set of configuration information defines a security association (SA) between the two VPN endpoints. When planning your VPN, you must make a few choices first:

- Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will either endpoint use Fully Qualified Domain Names (FQDNs)? FQDNs supplied by Dynamic DNS providers (see [“The Use of a Fully Qualified Domain Name \(FQDN\)” on page B-8](#)) can allow a VPN endpoint with a dynamic IP address to initiate or respond to a tunnel request. Otherwise, the side using a dynamic IP address must always be the initiator.
- What method will you use to configure your VPN tunnels?
 - The VPN Wizard using VPNC defaults (see [Table 6-2](#))
 - The typical automated Internet Key Exchange (IKE) setup (see [“Using Auto Policy to Configure VPN Tunnels” on page 6-36](#))
 - A Manual Keying setup in which you must specify each phase of the connection (see [“Using Manual Policy to Configure VPN Tunnels” on page 6-46](#))?

Table 6-2. Parameters Recommended by the VPNC and Used in the VPN Wizard

Parameter	Factory Default
Secure Association	Main Mode
Authentication Method	Pre-shared Key
Encryption Method	3DES
Authentication Protocol	SHA-1
Diffie-Hellman (DH) Group	Group 2 (1024 bit)
Key Life	8 hours
IKE Life Time	1 hour

- What level of IPSec VPN encryption will you use?
 - DES - The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
 - 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- What level of authentication will you use?

- MDS: 128 bits, faster but less secure.
- SHA-1: 160 bits, slower but more secure.



Note: NETGEAR publishes additional interoperability scenarios with various gateway and client software products. Look on the NETGEAR web site at www.netgear.com for these interoperability scenarios.

VPN Tunnel Configuration

There are two tunnel configurations and three ways to configure them:

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
 - See “[How to Set Up a Client-to-Gateway VPN Configuration](#)” on page 6-6.
 - See “[How to Set Up a Gateway-to-Gateway VPN Configuration](#)” on page 6-20.
- See “[Using Auto Policy to Configure VPN Tunnels](#)” on page 6-36 when the VPN Wizard and its VPNC defaults (see [Table 6-2 on page 6-4](#)) are not appropriate for your special circumstances, but you want to automate the Internet Key Exchange (IKE) setup.
- See “[Using Manual Policy to Configure VPN Tunnels](#)” on page 6-46 when the VPN Wizard and its VPNC defaults (see [Table 6-2 on page 6-4](#)) are not appropriate for your special circumstances and you must specify each phase of the connection. You manually enter all the authentication and key parameters. You have more control over the process, however the process is more complex and there are more opportunities for errors or configuration mismatches between your DG834 v3 and the corresponding VPN endpoint gateway or client workstation.

How to Set Up a Client-to-Gateway VPN Configuration

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway (see [Figure 6-3](#)) involves the following two steps:

- “[Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834 v3](#)” on page 6-6 uses the VPN Wizard to configure the VPN tunnel between the remote PC and network gateway.
- “[Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC](#)” on page 6-11 configures the NETGEAR ProSafe VPN Client endpoint.

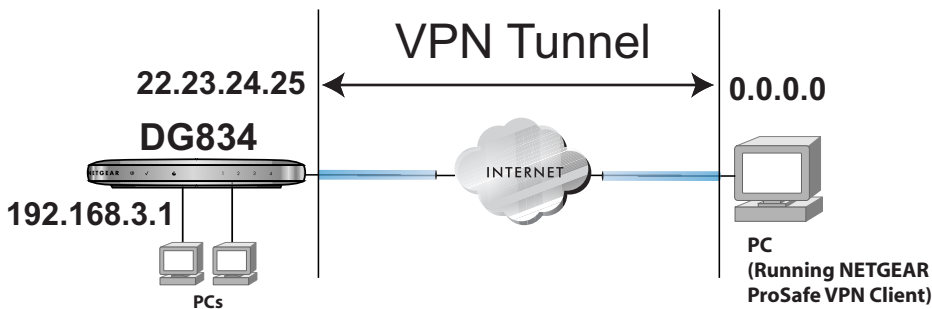


Figure 6-3

Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834 v3



Note: This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in [Table 6-2 on page 6-4](#). If you have special requirements not covered by these VPNC-recommended parameters, refer to “[How to Set Up VPN Tunnels in Special Circumstances](#)” on page 6-36 to set up the VPN tunnel.

The worksheet below identifies the parameters used in the following procedure. A blank worksheet is at “[Planning a VPN](#)” on page 6-3.

Table 6-1. VPN Tunnel Configuration Worksheet

Connection Name:	RoadWarrior			
Pre-Shared Key:	12345678			
Secure Association -- Main Mode or Manual Keys:	Main			
Perfect Forward Secrecy -- Enabled or Disabled:	Disabled			
Encryption Protocol -- DES or 3DES:	3DES			
Authentication Protocol -- MD5 or SHA-1:	SHA-1			
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	Group 2			
Key Life in seconds:	28800 (8 hours)			
IKE Life Time in seconds:	3600 (1 hour)			
VPN Endpoint	Local IPsec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
Client	toDG834	—	—	Dynamic
DG834 v3	toClient	192.168.3.1	255.255.255.0	22.23.24.25

Follow this procedure to configure a client-to-gateway VPN tunnel using the VPN Wizard.

1. Log in to the DG834 v3 at its LAN address of <http://192.168.0.1> with its default user name of **admin** and password of **password**. Click the VPN Wizard link in the main menu to display this screen. Click **Next** to proceed.

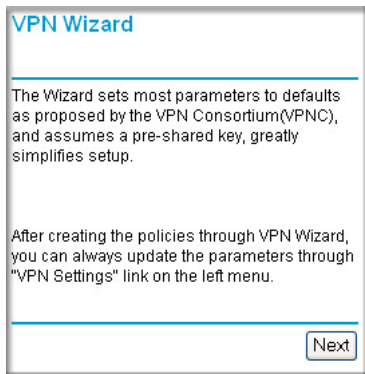
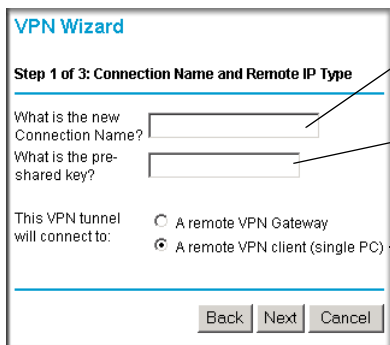
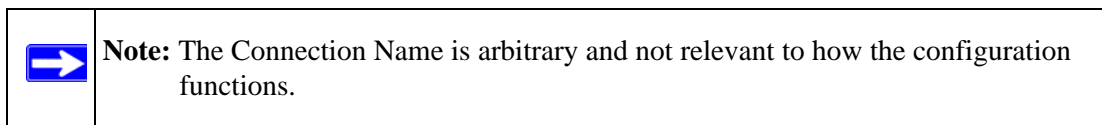


Figure 6-4

2. Fill in the Connection Name and the pre-shared key, select the type of target end point, and click **Next** to proceed.



Enter the new Connection Name:
(e.g., **RoadWarrior**)

Enter the pre-shared key:
(e.g., **12345678**)

Select the radio button:
A remote VPN client (single PC)

Figure 6-5

The Summary screen below displays.

VPN Wizard

Summary

Please verify your inputs:

Connection Name:	RoadWarrior
Remote VPN Endpoint:	Client PC
Remote Client Access:	Single PC - no Subnet
Remote IP:	Dynamic
Remote ID:	
Local Client Access:	By subnet
Local IP:	192.168.3.1 / 255.255.255.0
Local ID:	

You can click [here](#) to view the VPNC-recommended parameters.
Please click "**Done**" to apply the changes.

Figure 6-6

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the “**here**” link (see [Figure 6-6](#)). Click **Back** to return to the Summary screen.

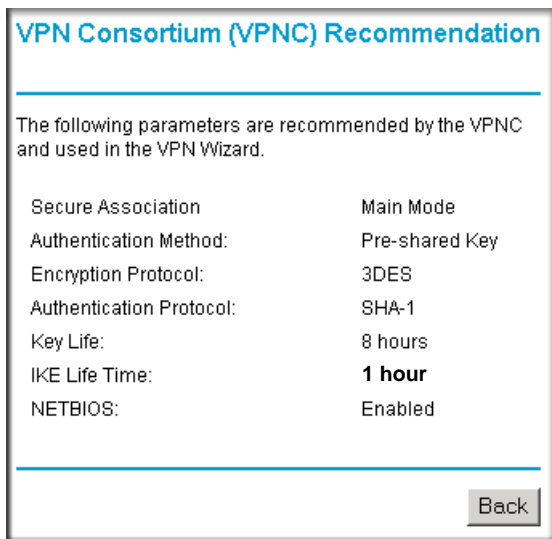


Figure 6-7

- Click **Done** on the Summary screen (see [Figure 6-6](#)) to complete the configuration procedure. The VPN Policies menu below displays showing that the new tunnel is enabled.

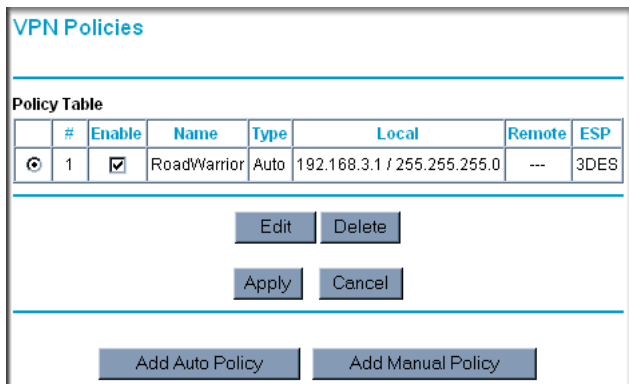


Figure 6-8

To view or modify the tunnel settings, select the radio button next to the tunnel entry and click Edit.



Note: Refer to “[Using Auto Policy to Configure VPN Tunnels](#)” on page 6-36 to enable the IKE keep-alive capability on an existing VPN tunnel.


Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC

This procedure describes how to configure the NETGEAR ProSafe VPN Client. We will assume the PC running the client has a dynamically assigned IP address.


The PC must have the NETGEAR ProSafe VPN Client program installed that supports IPsec. Go to the NETGEAR website (<http://www.netgear.com>) and select VPN01L_VPN05L in the Product Quick Find drop-down menu for information on how to purchase the NETGEAR ProSafe VPN Client.




Note: Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

1. Install the NETGEAR ProSafe VPN Client on the remote PC and reboot.
 - You may need to insert your Windows CD to complete the installation.
 - If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating “The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed.” You can disregard this message.
 - Install the IPsec Component. You may have the option to install either the VPN Adapter or the IPsec Component or both. The VPN Adapter is not necessary.
 - The system should show the ProSafe icon () in the system tray after rebooting.
 - Double-click the system tray icon to open the Security Policy Editor.
2. Add a new connection as follows:
 - a. Run the NETGEAR ProSafe Security Policy Editor program and, using the “[VPN Tunnel Configuration Worksheet](#)” on page 6-7, create a VPN Connection.

- b. From the Edit menu of the Security Policy Editor, click Add, then Connection. A “New Connection” listing appears in the list of policies. Rename the “New Connection” so that it matches the Connection Name you entered in the VPN Settings of the DG834 v3 on LAN A.

 **Note:** In this example, the Connection Name used on the client side of the VPN tunnel is **toDG834** and it does not have to match the **RoadWarrior** Connection Name used on the gateway side of the VPN tunnel (see [Figure 6-5](#)) because Connection Names are arbitrary to how the VPN tunnel functions.

 **Tip:** Choose Connection Names that make sense to the people using and administrating the VPN.

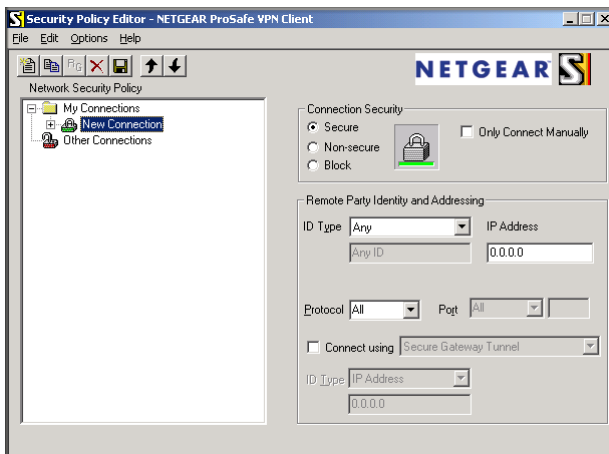


Figure 6-9

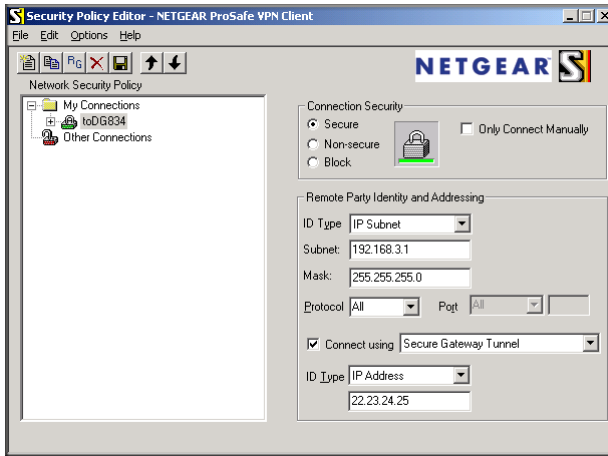


Figure 6-10

- c. Select the Secure in the Connection Security check box.
 - d. Select IP Subnet in the ID Type menu.
 - e. In this example, type **192.168.3.1** in the Subnet field as the network address of the DG834 v3.
 - f. Enter **255.255.255.0** in the Mask field as the LAN Subnet Mask of the DG834 v3.
 - g. Select All in the Protocol menu to allow all traffic through the VPN tunnel.
 - h. Select the Connect using Secure Gateway Tunnel check box.
 - i. Select IP Address in the ID Type menu below the check box.
 - j. Enter the public WAN IP Address of the DG834 v3 in the field directly below the ID Type menu. In this example, **22.23.24.25** would be used.
 - k. The resulting Connection Settings are shown in [Figure 6-10](#).
3. Configure the Security Policy in the NETGEAR ProSafe VPN Client software:
 - a. In the Network Security Policy list, expand the new connection by double clicking its name or clicking on the “+” symbol. My Identity and Security Policy subheadings appear below the connection name.

- b.** Click on the Security Policy subheading to show the Security Policy menu.

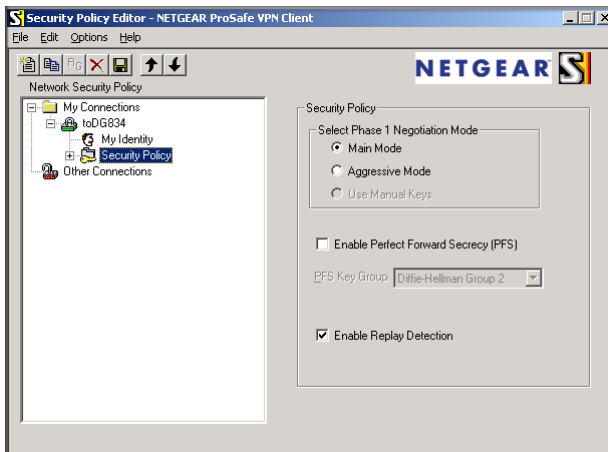


Figure 6-11

- c.** Select the Main Mode in the Select Phase 1 Negotiation Mode check box.
- 4.** Configure the VPN Client Identity.

In this step, you will provide information about the remote VPN client PC. You will need to provide the Pre-Shared Key that you configured in the DG834 v3 and either a fixed IP address or a “fixed virtual” IP address of the VPN client PC.

- a. In the Network Security Policy list on the left side of the Security Policy Editor window, click on My Identity.

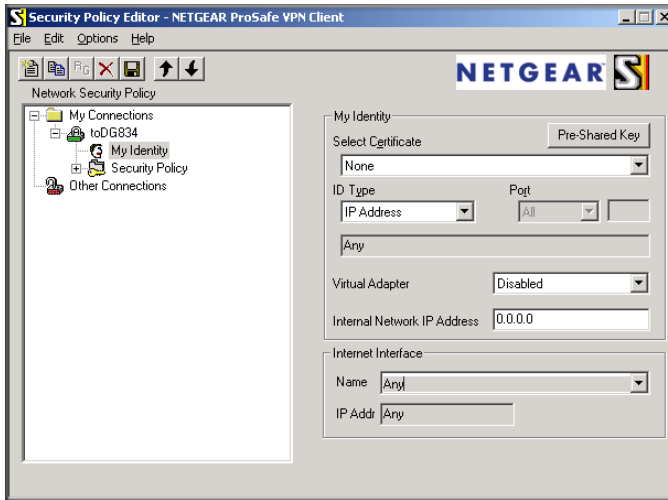


Figure 6-12

- b. Choose None in the Select Certificate menu.
- c. Select IP Address in the ID Type menu. If you are using a virtual fixed IP address, enter this address in the Internal Network IP Address box. Otherwise, leave this box empty.
- d. In the Internet Interface box, select the adapter you use to access the Internet. Select PPP Adapter in the Name menu if you have a dial-up Internet account. Select your Ethernet adapter if you have a dedicated Cable or DSL line. You may also choose Any if you will be switching between adapters or if you have only one adapter.
- e. Click the Pre-Shared Key button. In the Pre-Shared Key dialog box, click the Enter Key button. Enter the DG834 v3's Pre-Shared Key and click OK. In this example, **12345678** is entered. This field is case sensitive.

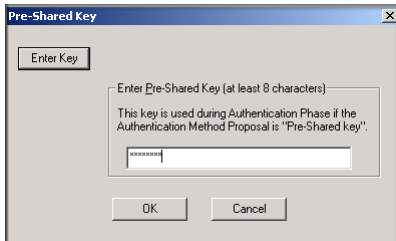


Figure 6-13

5. Configure the VPN Client Authentication Proposal.

In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the DG834 v3 configuration.

- a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double clicking its name or clicking on the “+” symbol.
- b. Expand the Authentication subheading by double clicking its name or clicking on the “+” symbol. Then select Proposal 1 below Authentication.

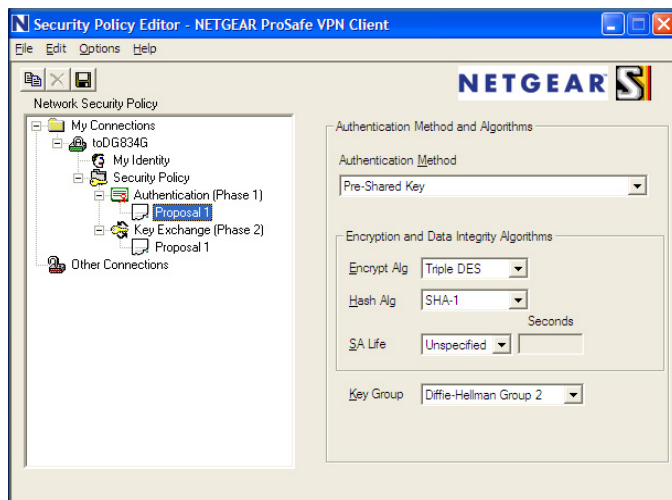


Figure 6-14

- c. In the Authentication Method menu, select Pre-Shared key.
 - d. In the Encrypt Alg menu, select the type of encryption to correspond with what was configured for the Encryption Protocol in the DG834 v3 in [Table 6-1 on page -7](#). In this example, use Triple DES.
 - e. In the Hash Alg menu, select SHA-1.
 - f. In the SA Life menu, select Unspecified.
 - g. In the Key Group menu, select Diffie-Hellman Group 2.
- ## 6. Configure the VPN Client Key Exchange Proposal.

In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the DG834 v3 configuration.

- a. Expand the Key Exchange subheading by double clicking its name or clicking on the “+” symbol. Then select Proposal 1 below Key Exchange.

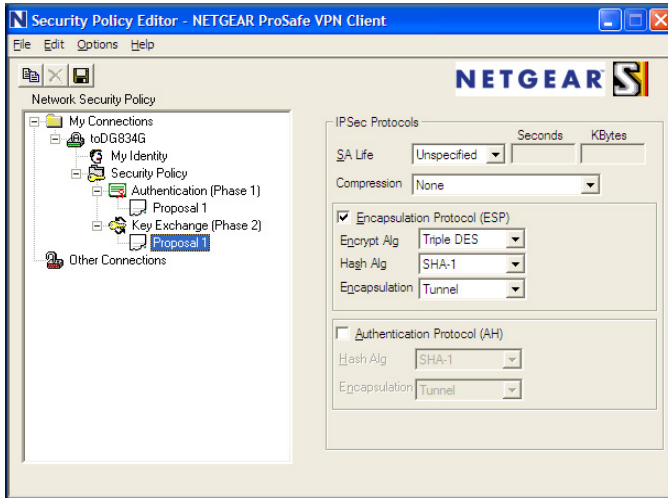


Figure 6-15

- b. In the SA Life menu, select Unspecified.
 - c. In the Compression menu, select None.
 - d. Check the Encapsulation Protocol (ESP) checkbox.
 - e. In the Encrypt Alg menu, select the type of encryption to correspond with what was configured for the Encryption Protocol in the DG834 v3 in [Table 6-1 on page -7](#). In this example, use Triple DES.
 - f. In the Hash Alg menu, select SHA-1.
 - g. In the Encapsulation menu, select Tunnel.
 - h. Leave the Authentication Protocol (AH) checkbox unchecked.
7. Save the VPN Client Settings.

From the File menu at the top of the Security Policy Editor window, select Save.

After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router’s LAN.

8. Check the VPN Connection.

To check the VPN Connection, you can initiate a request from the remote PC to the DG834 v3's network by using the "Connect" option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

To perform a ping test using our example, start from the remote PC:

- a. Establish an Internet connection from the PC.
- b. On the Windows taskbar, click the Start button, and then click Run.
- c. Type `ping -t 192.168.3.1` , and then click OK.

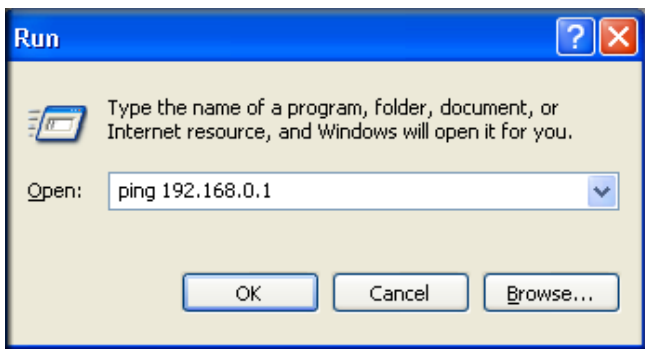


Figure 6-16

This will cause a continuous ping to be sent to the first DG834 v3. After between several seconds and two minutes, the ping response should change from "timed out" to "reply."

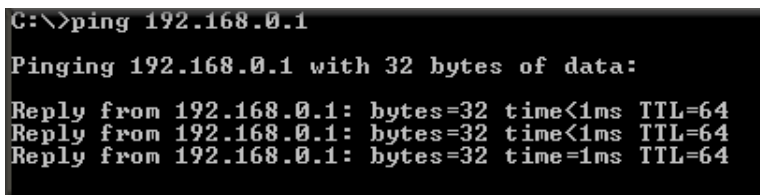


Figure 6-17

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the remote DG834 v3. After a short wait, you should see the login screen of the Modem Router (unless another PC already has the DG834 v3 management interface open).

Information on the progress and status of the VPN client connection can be viewed by opening the NETGEAR ProSafe Log Viewer.

1. To launch this function, click on the Windows Start button, then select Programs, then NETGEAR ProSafe VPN Client, then Log Viewer.
2. The Log Viewer screen for a successful connection is shown below:

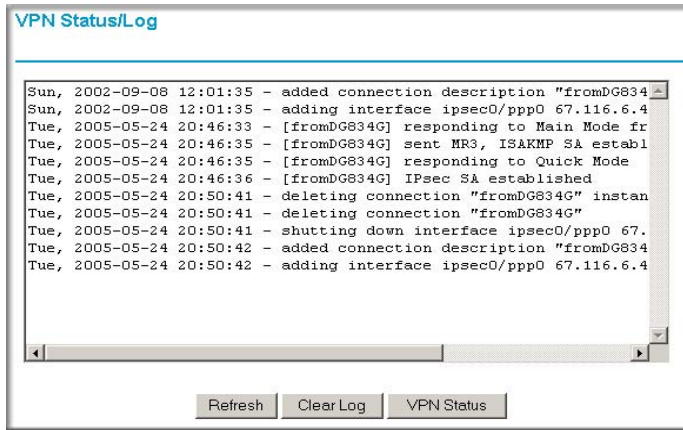


Figure 6-18



Note: Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

3. The Connection Monitor screen for this connection is shown below:

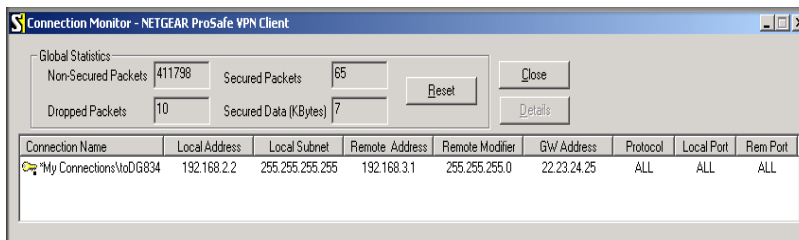


Figure 6-19

In this example you can see the following:

- The DG834 v3 has a public IP WAN address of 22.23.24.25.
- The DG834 v3 has a LAN IP address of 192.168.3.1.
- The VPN client PC has a dynamically assigned address of 192.168.2.2.

While the connection is being established, the Connection Name field in this menu will say “SA” before the name of the connection. When the connection is successful, the “SA” will change to the yellow key symbol shown in the illustration above.



Note: While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you will need to close the VPN connection in order to have normal Internet access.

How to Set Up a Gateway-to-Gateway VPN Configuration



Note: This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in [Table 6-2 on page -4](#). If you have special requirements not covered by these VPNC-recommended parameters, refer to [“How to Set Up VPN Tunnels in Special Circumstances” on page -36](#) to set up the VPN tunnel.

Follow this procedure to configure a gateway-to-gateway VPN tunnel using the VPN Wizard.

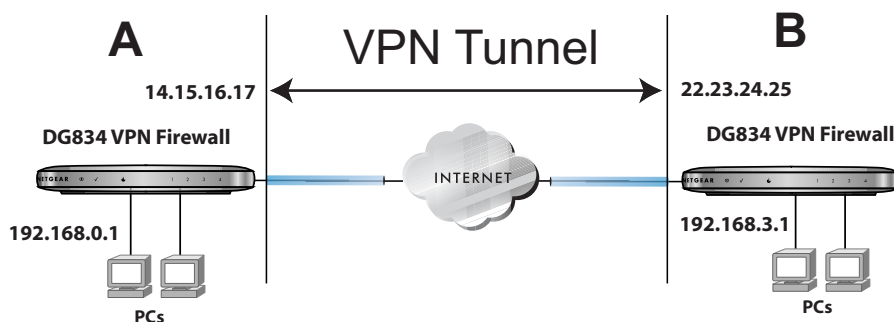


Figure 6-20

Set the LAN IPs on each DG834 v3 to different subnets and configure each properly for the Internet. The examples below assume the following settings:

Table 6-1. VPN Tunnel Configuration Worksheet

Connection Name:	GtoG			
Pre-Shared Key:	12345678			
Secure Association -- Main Mode or Manual Keys:	Main			
Perfect Forward Secrecy -- Enabled or Disabled:	Disabled			
Encryption Protocol -- DES or 3DES:	3DES			
Authentication Protocol -- MD5 or SHA-1:	SHA-1			
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	Group 2			
Key Life in seconds:	28800 (8 hours)			
IKE Life Time in seconds:	3600 (1 hour)			
				FQDN or Gateway IP (WAN IP Address)
VPN Endpoint	Local IPSec ID	LAN IP Address	Subnet Mask	
DG834 v3_A	GW_A	192.168.0.1	255.255.255.0	14.15.16.17
DG834 v3_B	GW_B	192.168.3.1	255.255.255.0	22.23.24.25



Note: The LAN IP address ranges of each VPN endpoint must be different. The connection will fail if both are using the NETGEAR default address range of 192.168.0.x.

Follow this procedure to configure a gateway-to-gateway VPN tunnel using the VPN Wizard.

1. Log in to the DG834 v3 on LAN A at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and password of **password**. Click the VPN Wizard link in the main menu to display this screen. Click **Next** to proceed.

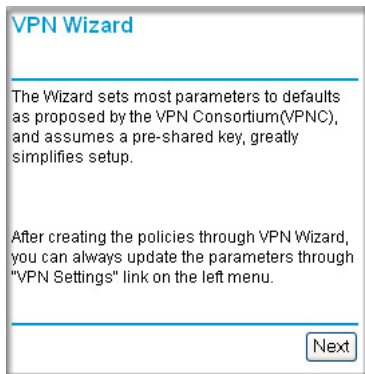


Figure 6-21

2. Fill in the Connection Name and the pre-shared key, select the type of target end point, and click **Next** to proceed.

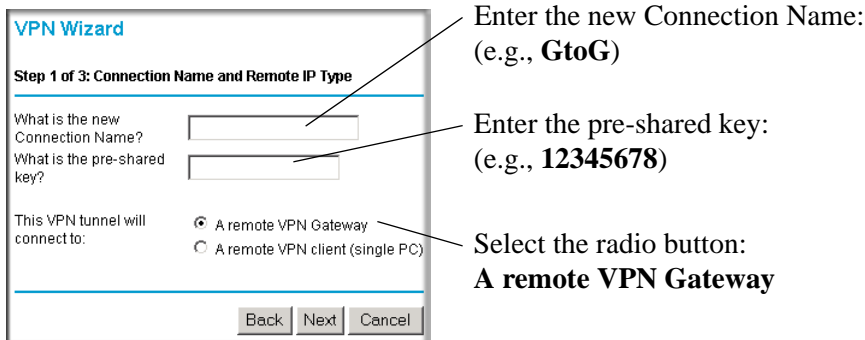


Figure 6-22

3. Fill in the IP Address or FQDN for the target VPN endpoint WAN connection and click **Next**.

VPN Wizard

Step 2 of 3: Remote IP address or the Internet name

What is the remote WAN's IP address or Internet name?

Enter the WAN IP address of the remote VPN gateway: (e.g., **22.23.24.25**)

Figure 6-23

4. Identify the IP addresses at the target endpoint which can use this tunnel, and click **Next**.

VPN Wizard

Step 3 of 3: Secure Connection Remote Accessibility

What is the **remote** LAN IP address and Subnet Mask?

IP Address: . . .

Subnet Mask: . . .

Enter the LAN IP settings of the remote VPN gateway:

- IP Address (e.g., **192.168.3.1**)
- Subnet Mask (e.g., **255.255.255.0**)

Figure 6-24

The Summary screen below displays.

The screenshot shows a web-based interface titled "VPN Wizard" with a "Summary" section. The summary lists the following configuration details:

Connection Name:	GtoG
Remote VPN Endpoint:	22.23.24.25
Remote Client Access:	By Subnet
Remote IP:	192.168.3.1 / 255.255.255.0
Remote ID:	
Local Client Access:	By subnet
Local IP:	192.168.0.1 / 255.255.255.0
Local ID:	

Below the summary, there is a note: "You can click [here](#) to view the VPNC-recommended parameters. Please click **\"Done\"** to apply the changes."

At the bottom right of the screen, there are three buttons: "Back", "Done", and "Cancel".

Figure 6-25

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the “**here**” link (see [Figure 6-25](#)). Click **Back** to return to the Summary screen.

VPN Consortium (VPNC) Recommendation

The following parameters are recommended by the VPNC and used in the VPN Wizard.

Secure Association	Main Mode
Authentication Method:	Pre-shared Key
Encryption Protocol:	3DES
Authentication Protocol:	SHA-1
Key Life:	8 hours
IKE Life Time:	1 hour
NETBIOS:	Enabled

Figure 6-26

- Click **Done** on the Summary screen (see [Figure 6-25](#)) to complete the configuration procedure. The VPN Settings menu below displays showing that the new tunnel is enabled.

VPN Policies

Policy Table


#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	GtoG	Auto	192.168.0.1 / 255.255.255.0	192.168.3.1 / 255.255.255.0	3DES

Figure 6-27



Note: Refer to “[Using Auto Policy to Configure VPN Tunnels](#)” on page 6-36 to enable the IKE keepalive capability on an existing VPN tunnel.

6. Repeat for the DG834 v3 on LAN B and pay special attention to use the following network settings as appropriate.
 - WAN IP of the remote VPN gateway (e.g., **14.15.16.17**)
 - LAN IP settings of the remote VPN gateway:
 - IP Address (e.g., **192.168.0.1**)
 - Subnet Mask (e.g., **255.255.255.0**)
 - Preshared Key (e.g., **12345678**)
7. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

	Note: The VPN Status screen is only one of three ways to active a VPN tunnel. See “Activating a VPN Tunnel” on page 6-27 for information on the other ways.
-----------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- a. Open the DG834 v3 management interface and click on VPN Status to get the VPN Status/Log screen ([Figure 6-28](#)).

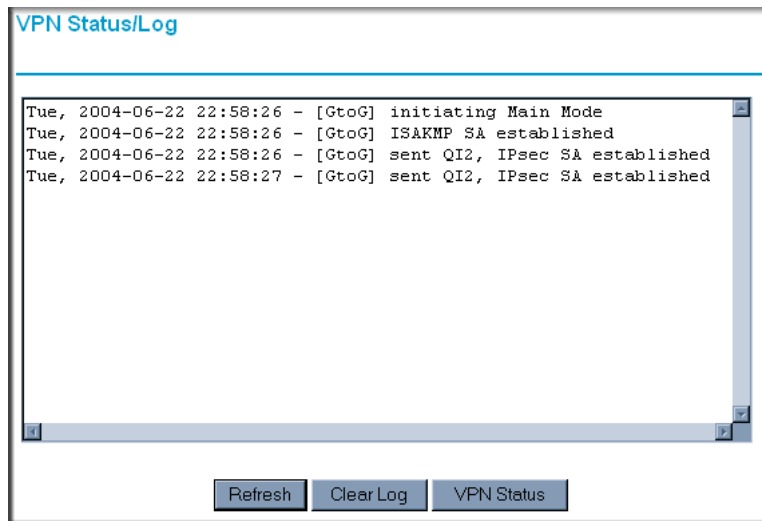


Figure 6-28

- b. Click on VPN Status ([Figure 6-30](#)) to get the Current VPN Tunnels (SAs) screen ([Figure 6-29](#)). Click on Connect for the VPN tunnel you want to activate.

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
2	---	---	GtoG	---	Connect	---	---

Figure 6-29

- c. Look at the VPN Status/Log screen ([Figure 6-28](#)) to verify that the tunnel is connected.

VPN Tunnel Control

Activating a VPN Tunnel

There are three ways to activate a VPN tunnel:

- Use the VPN Status page.
- Activate the VPN tunnel by pinging the remote endpoint.
- Start using the VPN tunnel.



Note: Refer to [“Using Auto Policy to Configure VPN Tunnels”](#) on page 6-36 to enable the IKE keepalive capability on an existing VPN tunnel.

Using the VPN Status Page to Activate a VPN Tunnel

To use the VPN Status screen to activate a VPN tunnel, perform the following steps:

1. Log in to the Modem Router.
2. Open the DG834 v3 management interface and click on VPN Status to get the VPN Status/Log screen (Figure 6-30).

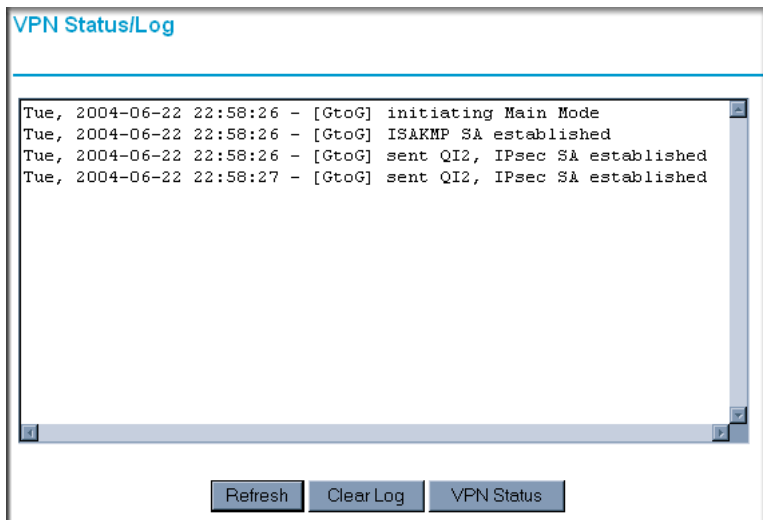


Figure 6-30

3. Click on VPN Status (Figure 6-30) to get the Current VPN Tunnels (SAs) screen (Figure 6-31). Click on Connect for the VPN tunnel you want to activate.

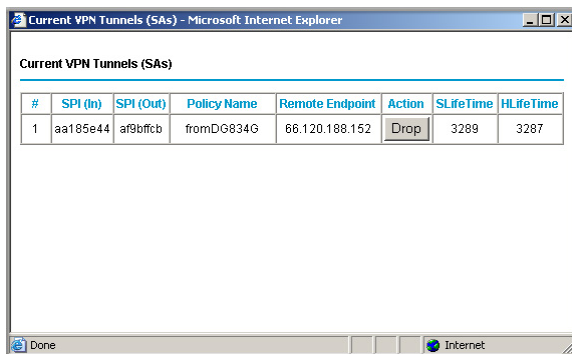


Figure 6-31

Activate the VPN Tunnel by Pinging the Remote Endpoint



Note: This section uses 192.168.3.1 for an example remote endpoint LAN IP address.

To activate the VPN tunnel by pinging the remote endpoint (e.g., 192.168.3.1), do the following steps depending on whether your configuration is client-to-gateway or gateway-to-gateway:

- **Client-to-Gateway Configuration**—to check the VPN Connection, you can initiate a request from the remote PC to the DG834 v3's network by using the “Connect” option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

To perform a ping test using our example, start from the remote PC:

- a. Establish an Internet connection from the PC.
- b. On the Windows taskbar, click the Start button, and then click Run.
- c. Type `ping -t 192.168.3.1` and then click OK.

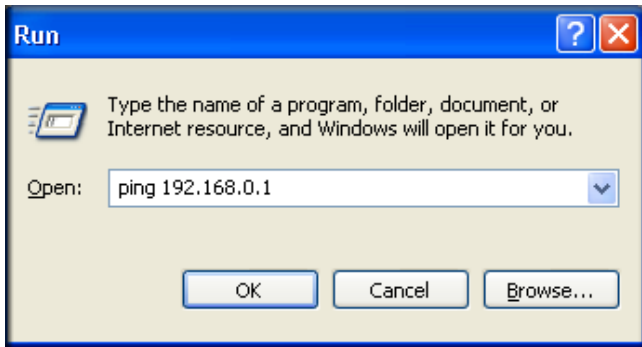


Figure 6-32

This will cause a continuous ping to be sent to the first DG834 v3. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.”



Note: Use **Ctrl-C** to stop the pinging.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
```

Figure 6-33

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the remote DG834 v3. After a short wait, you should see the login screen of the Modem Router (unless another PC already has the DG834 v3 management interface open).

- **Gateway-to-Gateway Configuration**—test the VPN tunnel by pinging the remote network from a PC attached to the DG834 v3.
 - a. Open command prompt (i.e., Start -> Run -> cmd).
 - b. ping 192.168.3.1.

```
Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=10ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
```

Figure 6-34

Note: The pings may fail the first time. If so, then try the pings a second time.

Start Using a VPN Tunnel to Active It

To use a VPN tunnel, use a Web browser to go to a URL whose IP address or range is covered by the policy for that VPN tunnel.

Verifying the Status of a VPN Tunnel

To use the VPN Status page to determine the status of a VPN tunnel, perform the following steps:

1. Log in to the Modem Router.
2. Open the DG834 v3 management interface and click on VPN Status to get the VPN Status/Log screen ([Figure 6-35](#)).

Log—this log shows the details of recent VPN activity, including the building of the VPN tunnel. If there is a problem with the VPN tunnel, refer to the log for information about what might be the cause of the problem.

- Click Refresh to see the most recent entries.
- Click Clear Log to delete all log entries.

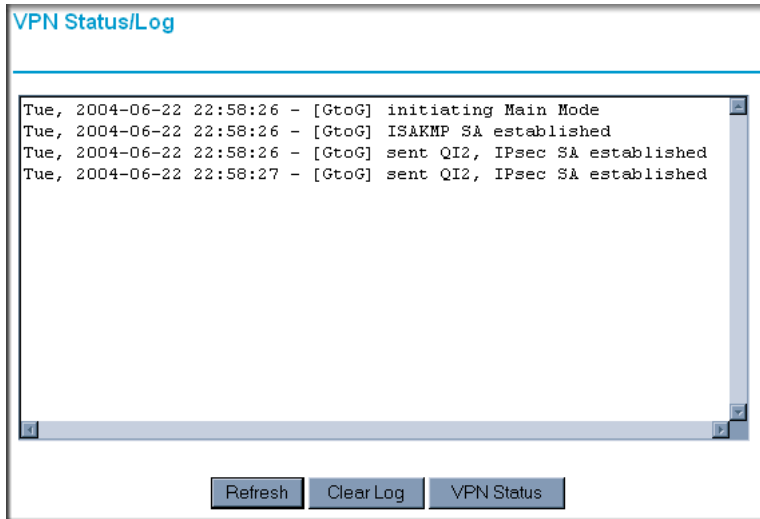


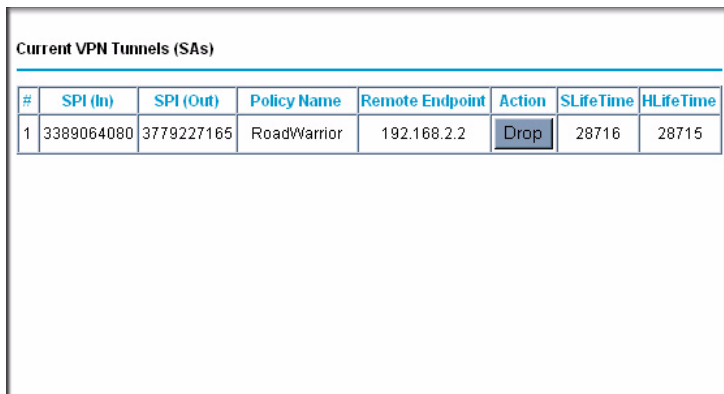
Figure 6-35

3. Click on VPN Status (Figure 6-30) to get the Current VPN Tunnels (SAs) screen (Figure 6-31).

This table lists the following data for each active VPN Tunnel.

- **SPI**—each SA has a unique SPI (Security Parameter Index) for traffic in each direction. For "Manual" key exchange, the SPI is specified in the Policy definition. For "Automatic" key exchange, the SPI is generated by the IKE protocol.
- **Policy Name**—the name of the VPN policy associated with this SA.
- **Remote Endpoint**—the IP address on the remote VPN Endpoint.
- **Action**—the action will be either a "Drop" or a "Connect" button.
- **SLifeTime (Secs)**—the remaining Soft Lifetime for this SA in seconds. When the Soft Lifetime becomes zero, the SA (Security Association) will re-negotiated.

- **HLifeTime (Secs)**—the remaining Hard Lifetime for this SA in seconds. When the Hard Lifetime becomes zero, the SA (Security Association) will be terminated. (It will be re-established if required.)



The screenshot shows a web interface titled "Current VPN Tunnels (SAs)". Below the title is a table with the following data:

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	3389064080	3779227165	RoadWarrior	192.168.2.2	Drop	28716	28715

Figure 6-36

Deactivating a VPN Tunnel

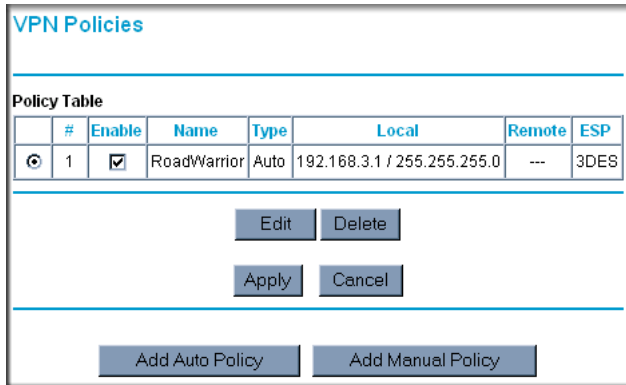
Sometimes a VPN tunnel must be deactivated for testing purposes. There are two ways to deactivate a VPN tunnel:

- Policy table on VPN Policies page
- VPN Status page

Using the Policy Table on the VPN Policies Page to Deactivate a VPN Tunnel

To use the VPN Policies page to deactivate a VPN tunnel, perform the following steps:

1. Log in to the Modem Router.
2. Open the DG834 v3 management interface and click on VPN Policies to get the VPN Policies screen (Figure 6-38).



The screenshot shows the 'VPN Policies' page. At the top, there is a 'Policy Table' with the following data:

	#	Enable	Name	Type	Local	Remote	ESP
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	RoadWarrior	Auto	192.168.3.1 / 255.255.255.0	---	3DES

Below the table are two rows of buttons: 'Edit' and 'Delete' in the first row, and 'Apply' and 'Cancel' in the second row. At the bottom of the page are two buttons: 'Add Auto Policy' and 'Add Manual Policy'.

Figure 6-37

3. Clear the Enable check box for the VPN tunnel you want to deactivate and click Apply. (To reactivate the tunnel, check the Enable box and click Apply.)

Using the VPN Status Page to Deactivate a VPN Tunnel

To use the VPN Status page to deactivate a VPN tunnel, perform the following steps:

1. Log in to the Modem Router.

- Open the DG834 v3 management interface and click on VPN Status to get the VPN Status/Log screen (Figure 6-38).

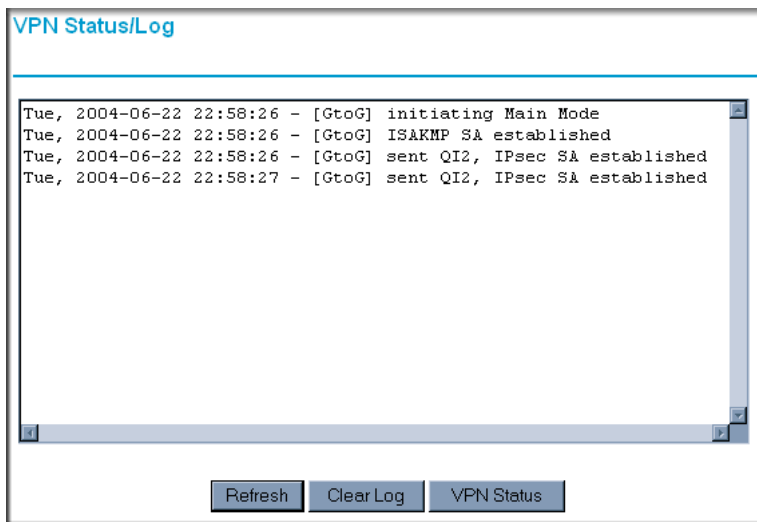


Figure 6-38

- Click VPN Status (Figure 6-38) to get the Current VPN Tunnels (SAs) screen (Figure 6-39). Click Drop for the VPN tunnel you want to deactivate.

The screenshot shows a window titled "Current VPN Tunnels (SAs)". It contains a table with the following data:

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	3389064080	3779227165	RoadWarrior	192.168.2.2	Drop	28716	28715

Figure 6-39

Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the Modem Router.
2. Open the DG834 v3 management interface and click VPN Policies to display the VPN Policies screen (Figure 6-40). Select the radio button for the VPN tunnel to be deleted and click the Delete button.

#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	RoadWarrior	Auto	192.168.3.1 / 255.255.255.0	---	3DES

Figure 6-40

How to Set Up VPN Tunnels in Special Circumstances

When the VPN Wizard and its VPNC defaults (see [Table 6-2](#)) are not appropriate for your special circumstances, use one of the following alternatives:

- **Auto Policy**—for a typical automated Internet Key Exchange (IKE) setup, see [“Using Auto Policy to Configure VPN Tunnels” on page 6-36](#). Auto Policy uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys.
- **Manual Policy**—for a Manual Keying setup in which you must specify each phase of the connection, see [“Using Manual Policy to Configure VPN Tunnels” on page 6-46](#). Manual Policy does not use IKE. Rather, you manually enter all the authentication and key parameters. You have more control over the process, however the process is more complex and there are more opportunities for errors or configuration mismatches between your DG834 v3 and the corresponding VPN endpoint gateway or client workstation.

Using Auto Policy to Configure VPN Tunnels

You need to configure matching VPN settings on both VPN endpoints. The outbound VPN settings on one end must match to the inbound VPN settings on other end, and vice versa.

See [“Example of Using Auto Policy” on page 6-41](#) for an example of using Auto Policy.

Configuring VPN Network Connection Parameters

All VPN tunnels on the DG834 ADSL Modem Router require configuring several network parameters. This section describes those parameters and how to access them.

The most common configuration scenarios will use IKE to manage the authentication and encryption keys. The IKE protocol performs negotiations between the two VPN endpoints to automatically generate and update the required encryption parameters.

Click the VPN Policies link of the main menu, and then click the Add Auto Policy button to display the VPN - Auto Policy menu shown in [Figure 6-41](#).

Policy Table						
#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	toClient	Auto	192.168.0.0 / 255.255.255.0	---	3DES
2	<input type="checkbox"/>	ToFVL	Auto	192.168.0.0 / 255.255.255.0	192.168.2.0 / 255.255.255.0	3DES

VPN - Auto Policy

General

Policy Name:

Remote VPN Endpoint: Address Type: Address Data:

NetBIOS Enable
 IKE Keep Alive

Ping IP Address: . . .

Local LAN

IP Address:

Single/Start address: . . .

Finish address: . . .

Subnet Mask: . . .

Remote LAN

IP Address:

Single/Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

IKE

Direction:

Exchange Mode:

Diffie-Hellman (DH) Group:

Local Identity Type:

Data:

Remote Identity Type:

Data:

Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-shared Key:

SA Life Time: (Seconds)

Enable PFS (Perfect Forward Security)

Figure 6-41

The DG834 v3 VPN tunnel network connection fields are defined as follows:

General. These settings identify this policy and determine its major characteristics.

- **Policy Name**—Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**—If the remote endpoint has a dynamic IP address, select "Dynamic IP address". No "Address Data" input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select the desired option (IP address or Domain Name) and enter the address of the remote VPN endpoint to which you wish to connect.



Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".

- **IKE Keep-alive**—Enable this if you wish to ensure that a connection is kept open, or, if that is not possible, that it is quickly re-established when disconnected.

The Ping IP Address must be associated with the remote endpoint. The remote LAN address must be used. This IP address will be "pinged" periodically to generate traffic for the VPN tunnel. The remote keep-alive IP address must be covered by the remote LAN IP range and must correspond to a device that can respond to ping. The range should be made as narrow as possible to meet this objective.

Local LAN. This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single address**—enter an IP address in the "Single/Start IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on your LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field. The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.

Remote LAN. This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single PC - no Subnet**—select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. The typical application is a PC running the VPN client at the remote end.
- **Single address**—Enter an IP address in the "Single/Start IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on the remote LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.

The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.

IKE. Direction/Type—this setting is used when determining if the IKE policy matches the current traffic. Select the desired option.

- **Responder only**—incoming connections are allowed, but outgoing connections will be blocked.
- **Initiator and Responder**—both incoming and outgoing connections are allowed.

Exchange Mode—ensure the remote VPN endpoint is set to use "Main Mode".

Diffie-Hellman (DH) Group—the Diffie-Hellman algorithm is used when exchanging keys. The DH Group setting determines the number of bit size used in the exchange. This value must match the value used on the remote VPN Gateway.

Local Identity Type—select the desired option to match the "Remote Identity Type" setting on the remote VPN endpoint.

- **WAN IP Address**—your Internet IP address.
- **Fully Qualified Domain Name**—your domain name.
- **Fully Qualified User Name**—your name, E-mail address, or other ID.

Local Identity Data—enter the data for the selection above. (If "WAN IP Address" is selected, no input is required.)

Remote Identity Type—select the desired option to match the "Local Identity Type" setting on the remote VPN endpoint.

- **IP Address**—the Internet IP address of the remote VPN endpoint.
- **Fully Qualified Domain Name**—the Domain name of the remote VPN endpoint.

- **Fully Qualified User Name**—the name, E-mail address, or other ID of the remote VPN endpoint.

Remote Identity Data—enter the data for the selection above. (If "IP Address" is selected, no input is required.)

Parameters. Encryption Algorithm—encryption Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway. DES and 3DES are supported.

- DES—the Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
- 3DES—(Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

Authentication Algorithm—authentication Algorithm used for both IKE and IPSec. This setting must match the setting used on the remote VPN Gateway. Auto, MD5, and SHA-1 are supported. Auto negotiates with the remote VPN endpoint and is not available in responder-only mode.

- MD5—128 bits, faster but less secure.
- SHA-1 (default)—160 bits, slower but more secure.

Pre-shared Key—the key must be entered both here and on the remote VPN Gateway.

SA Life Time—this determines the time interval before the SA (Security Association) expires. (It will automatically be re-established as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA Life Time. This setting applies to both IKE and IPSec SAs.

IPSec PFS (Perfect Forward Secrecy)—if enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you may have to specify the "Key Group" used. For this device, the "Key Group" is the same as the "DH Group" setting in the IKE section.

Example of Using Auto Policy

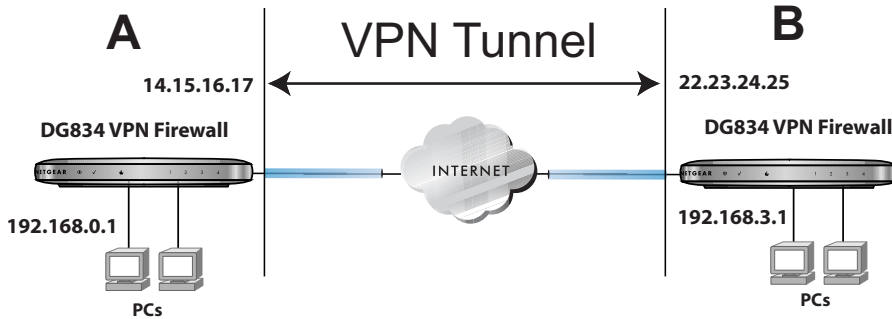


Figure 6-42

1. Set the LAN IPs on each DG834 v3 to different subnets and configure each properly for the Internet. The following settings are assumed for this example:

Table 6-1. VPN Tunnel Configuration Worksheet

Connection Name:	GtoG			
Pre-Shared Key:	12345678			
Secure Association -- Main Mode or Manual Keys:	Main			
Perfect Forward Secrecy -- Enabled or Disabled:	Disabled			
Encryption Protocol -- DES or 3DES:	3DES			
Authentication Protocol -- MD5 or SHA-1:	SHA-1			
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	Group 2			
Key Life in seconds:	28800 (8 hours)			
IKE Life Time in seconds:	3600 (1 hour)			
				FQDN or Gateway IP (WAN IP Address)
VPN Endpoint	Local IPsec ID	LAN IP Address	Subnet Mask	
DG834 v3 A	LAN_A	192.168.0.1	255.255.255.0	14.15.16.17
DG834 v3 B	LAN_B	192.168.3.1	255.255.255.0	22.23.24.25

- Open the DG834 v3 on LAN A management interface and click on VPN Policies.

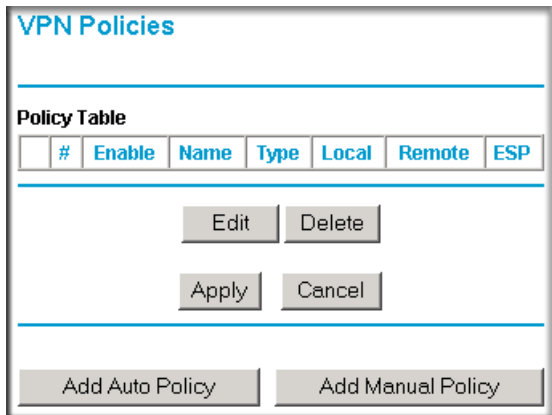


Figure 6-43

- Click Add Auto Policy.
- Enter policy settings (see [Figure 6-44](#)).
 - General
 - Policy Name = GtoG
 - Remote VPN Endpoint Address Type = Fixed IP Address
 - Remote VPN Endpoint Address Data = 22.23.24.25
 - Local LAN – use default setting
 - Remote LAN
 - IP Address = select Subnet address from the pulldown menu.
 - Start IP address = 192.168.3.1
 - Subnet Mask = 255.255.255.0
 - IKE
 - Direction = Initiator and Responder
 - Exchange Mode = Main Mode
 - Diffie-Hellman (DH) Group = Group 2 (1024 Bit)
 - Local Identity Type = use default setting
 - Remote Identity Type = use default setting
 - Parameters
 - Encryption Algorithm = 3DES
 - Authentication Algorithm = MD5

— Pre-shared Key = 12345678

VPN - Auto Policy

General

Policy Name:

Remote VPN Endpoint: Address Type: Address Data:

NetBIOS Enable

IKE Keep Alive

Ping IP Address:

Local LAN

IP Address:

Single/Start address:

Finish address:

Subnet Mask:

Remote LAN

IP Address:

Single/Start IP address:

Finish IP address:

Subnet Mask:

IKE

Direction:

Exchange Mode:

Diffie-Hellman (DH) Group:

Local Identity Type:

Data:

Remote Identity Type:

Data:

Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-shared Key:

SA Life Time: (Seconds)

Enable PFS (Perfect Forward Security)

Figure 6-44

5. Click Apply. The Get VPN Policies web page is displayed.

VPN Policies						
Policy Table						
#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	GtoG	Auto	192.168.0.1 / 255.255.255.0	192.168.3.1 / 255.255.255.0	3DES

Figure 6-45

6. Repeat for the DG834 v3 on LAN B and pay special attention to use the following network settings as appropriate.
- General, Remote Address Data (e.g., **14.15.16.17**)
 - Remote LAN, Start IP Address
 - IP Address (e.g, **192.168.0.1**)
 - Subnet Mask (e.g., **255.255.255.0**)
 - Preshared Key (e.g., **12345678**)
7. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:



Note: The VPN Status screen is only one of three ways to activate a VPN tunnel. See [“Activating a VPN Tunnel” on page 6-27](#) for information on the other ways.

- a. Open the DG834 v3 management interface and click on VPN Status to display the VPN Status/Log screen (Figure 6-46).

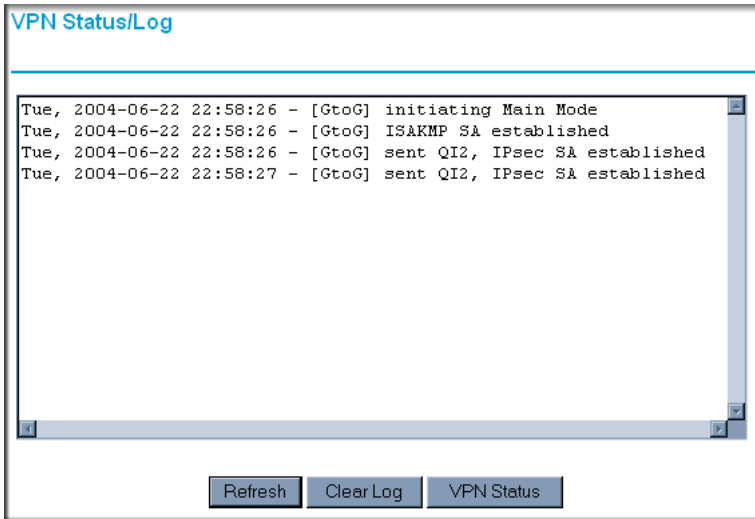


Figure 6-46

- b. Click VPN Status (Figure 6-46) to display the Current VPN Tunnels (SAs) screen (Figure 6-47). Click on Connect for the VPN tunnel you want to activate.

The screenshot shows a window titled "Current VPN Tunnels (SAs)". It contains a table with the following data:

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
2	---	---	GtoG	---	Connect	---	---

Figure 6-47

- c. Review the VPN Status/Log screen (Figure 6-46) to verify that the tunnel is connected.

Using Manual Policy to Configure VPN Tunnels

As an alternative to IKE, you may use Manual Keying, in which you must specify each phase of the connection. A "Manual" VPN policy requires all settings for the VPN tunnel to be manually input at each end (both VPN endpoints).

Click the VPN Policies link of the main menu, and then click the Add Manual Policy radio button to display the Manual Keys menu shown in [Figure 6-48](#).

VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	toClient	Auto	192.168.0.0 / 255.255.255.0	---	3DES
2	<input type="checkbox"/>	ToFVL	Auto	192.168.0.0 / 255.255.255.0	192.168.2.0 / 255.255.255.0	3DES

Buttons: Edit, Delete, Apply, Cancel, Add Auto Policy, Add Manual Policy

VPN - Manual Policy

General

Policy Name:

Remote VPN Endpoint Address Type: Fixed IP Address

Address Data:

NETBIOS Enable

Local LAN

IP Address: Subnet address

Single/Start address: 192 . 168 . 0 . 1

Finish address: . . .

Subnet Mask: 255 . 255 . 255 . 0

Remote LAN

IP Address: Single PC - no subnet

Single/Start IP address: . . .

Finish IP address: . . .

Subnet Mask: . . .

ESP Configuration

SPI - Incoming: (Hex, 3 Characters)

SPI - Outgoing: (Hex, 3 Characters)

Encryption: 3DES

Key:
(DES - 8 chars; 3DES - 24 chars)

Authentication: SHA-1

Key:
(MD5 - 16 chars; SHA-1 - 20 chars)

Buttons: Back, Apply, Cancel

Figure 6-48

General. The DG834 v3 VPN tunnel network connection fields are defined as follows:

- **Policy Name**—enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.

- **Remote VPN Endpoint**—select the desired option (IP address or Fully Qualified Domain Name) and enter the address of the remote VPN endpoint to which you wish to connect.

Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".

Local LAN. This identifies which PCs on your LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single address**—enter an IP address in the "Single/Start IP address" field. Typically, this setting is used when you wish to make a single Server on your LAN available to remote users.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on your LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.

The remote VPN endpoint must have these IP addresses entered as its "Remote" addresses.

Remote LAN. This identifies which PCs on the remote LAN are covered by this policy. For each selection, data must be provided as follows:

- **Single PC - no Subnet**—select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required.
- **Single address**—enter an IP address in the "Single/Start IP address" field. This must be an address on the remote LAN. Typically, this setting is used when you wish to access a server on the remote LAN.
- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on the remote LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.

The remote VPN endpoint must have these IP addresses entered as its "Local" addresses.

ESP Configuration. ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel.

SPI—enter the required security policy indexes (SPIs). Each policy must have unique SPIs. These settings must match the remote VPN endpoint. The "in" setting here must match the "out" setting on the remote VPN endpoint, and the "out" setting here must match the "in" setting on the remote VPN endpoint.

Encryption—select the desired Encryption Algorithm, and enter the key in the field provided. For 3DES, the keys should be 24 ASCII characters and for DES, the keys should be 8 ASCII characters.

- DES—the Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
- 3DES—(Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.

Authentication—select the desired SHA-1 or MD5 Authentication Algorithm, and enter the key in the field provided. For MD5, the keys should be 16 ASCII characters. For SHA-1, the keys should be 20 ASCII characters.

- MD5—128 bits, faster but less secure.
- SHA-1 (default)—160 bits, slower but more secure.

Chapter 7

Troubleshooting

This chapter gives information about troubleshooting your DG834 ADSL Modem Router. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?
- Have I connected the router correctly?
Go to [“Basic Functioning” on page 7-1](#).
- I can’t access the router’s configuration with my browser.
Go to [“Troubleshooting the Web Configuration Interface” on page 7-3](#).
- I’ve configured the router but I can’t access the Internet.
Go to [“Troubleshooting the ISP Connection” on page 7-4](#).
- I can’t remember the router’s configuration password.
Go to [“Restoring the Default Configuration and Password” on page 7-9](#).
- I want to clear the configuration and start over again.
Go to [“Restoring the Default Configuration and Password” on page 7-9](#).

Basic Functioning

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

1. When power is first applied, verify that the Power LED is on (see [“The Modem Router’s Front Panel” on page 2-7](#) 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 7-9](#).

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

LAN or Internet Port LEDs Not On

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

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.

- Be sure you are using the correct cable:
 - When connecting the router's WAN ADSL port, use the cable that was supplied with the DG834 v3.

Troubleshooting the Web Configuration Interface

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

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



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

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in [“Using the Reset button” on page 7-9](#).
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.

- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

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

ADSL link

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

Internet LED Green or Blinking Green

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

Internet LED Blinking Amber

If your Internet LED is blinking amber, then your 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 DG834 ADSL Modem Router 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 an 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 *ADSL Modem Router Setup Manual* for details (see [Table 2-1 on page 2-9](#)).

Troubleshooting PPPoE or PPPoA

The PPPoE 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 C](#). 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 C](#).

Troubleshooting a TCP/IP Network Using the Ping Utility

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

Testing the LAN Path to Your Router

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

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

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

```
ping 192.168.0.1
```

3. Click OK.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

Request timed out

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

- Wrong physical connections
 - Make sure the LAN port LED is on. If the LED is off, follow the instructions in [“LAN or Internet Port LEDs Not On”](#) on page 7-2.
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
 - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

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

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

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

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

- Check that your PC has the IP address of your router listed as the default 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 C](#).
- 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 the *ADSL Modem Router Setup Manual* for details (see [Table 2-1 on page 2-9](#)).

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 4-1](#)).
- 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 DG834 ADSL Modem Router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

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

Appendix A

Technical Specifications

This appendix provides technical specifications for the DG834 ADSL Modem Router.

Network Protocol and Standards Compatibility

Data and Routing Protocols: TCP/IP, RIP-1, RIP-2, DHCP, PPP over Ethernet (PPPoE) or PPP over ATM (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, ADSL2+, Dual RJ-11, pins 2 and 3
T1.413, G.DMT, G.Lite
ITU Annex A or B (Annex B unit is DG834B)

Appendix B

NETGEAR VPN Configuration

DG834 v3 to FVL328

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DG834 v3 to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>).

Configuration Profile

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

Table B-1. Profile Summary

VPN Consortium Scenario:	Scenario 1
Type of VPN	LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:	IKE with Preshared Secret/Key (not Certificate-based)
IP Addressing:	
NETGEAR-Gateway A	Static IP address
NETGEAR-Gateway B	Static IP address

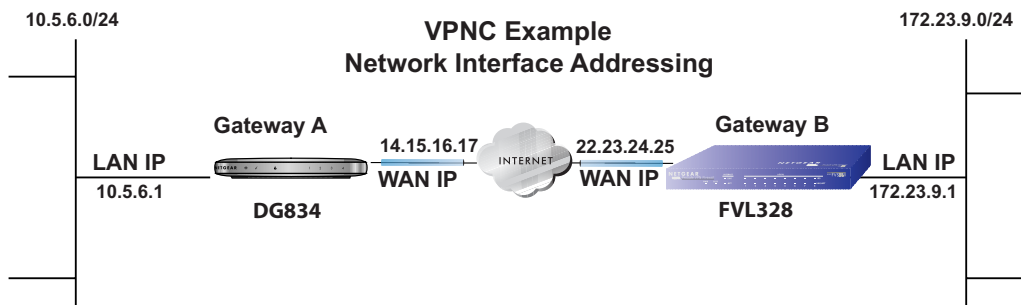


Figure B-1



Note: Product updates are available on the NETGEAR, Inc. web site at [http://kbserver.netgear.com/DG834 v3.asp](http://kbserver.netgear.com/DG834%20v3.asp).

Step-By-Step Configuration

1. Configure the DG834 v3 as in the Gateway-to-Gateway procedures using the VPN Wizard (see “[How to Set Up a Gateway-to-Gateway VPN Configuration](#)” on page 6-20), being certain to use appropriate network addresses for the environment.

The LAN Addresses used in this example are as follows:

Device	WAN IP Address	LAN IP Address	LAN Subnet Mask
DG834 v3	14.15.16.17	10.5.6.1	255.255.255.0
FVL328	22.23.24.25	172.23.9..1	255.255.255.0

- a. In Step 1, enter **toFVL328** for the Connection Name.
- b. In Step 2, enter **22.23.24.25** for the remote WAN's IP address.
- a. In Step 3, enter the following:
 - IP Address = **172.23.9.1**
 - Subnet Mask = **255.255.255.0**

VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	toFVL328	Auto	10.5.6.1 / 255.255.255.0	172.23.9.1 / 255.255.255.0	3DES

Click VPN Policies under Advanced - VPN to invoke this screen

VPN - Auto Policy

General

Policy Name:

Remote VPN Endpoint

Address Type:

Address Data:

NetBIOS Enable
 IKE Keep Alive

Ping IP Address:

Local LAN

IP Address:

Single/Start address:

Finish address:

Subnet Mask:

Remote LAN

IP Address:

Single/Start IP address:

Finish IP address:

Subnet Mask:

IKE

Direction:

Exchange Mode:

Diffie-Hellman (DH) Group:

Local Identity Type:

Data:

Remote Identity Type:

Data:

Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-shared Key:

SA Life Time: (Seconds)

Enable PFS (Perfect Forward Security)

Figure B-2

2. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see [“How to Set Up a Gateway-to-Gateway VPN Configuration”](#) on page 6-20), being certain to use appropriate network addresses for the environment.
 - a. In Step 1, enter **toDG834** for the Connection Name
 - b. In Step 2, enter **14.15.16.17** for the remote WAN's IP address
 - c. In Step 3, enter the following:
 - IP Address = **10.5.6.1**
 - Subnet Mask = **255.255.255.0**

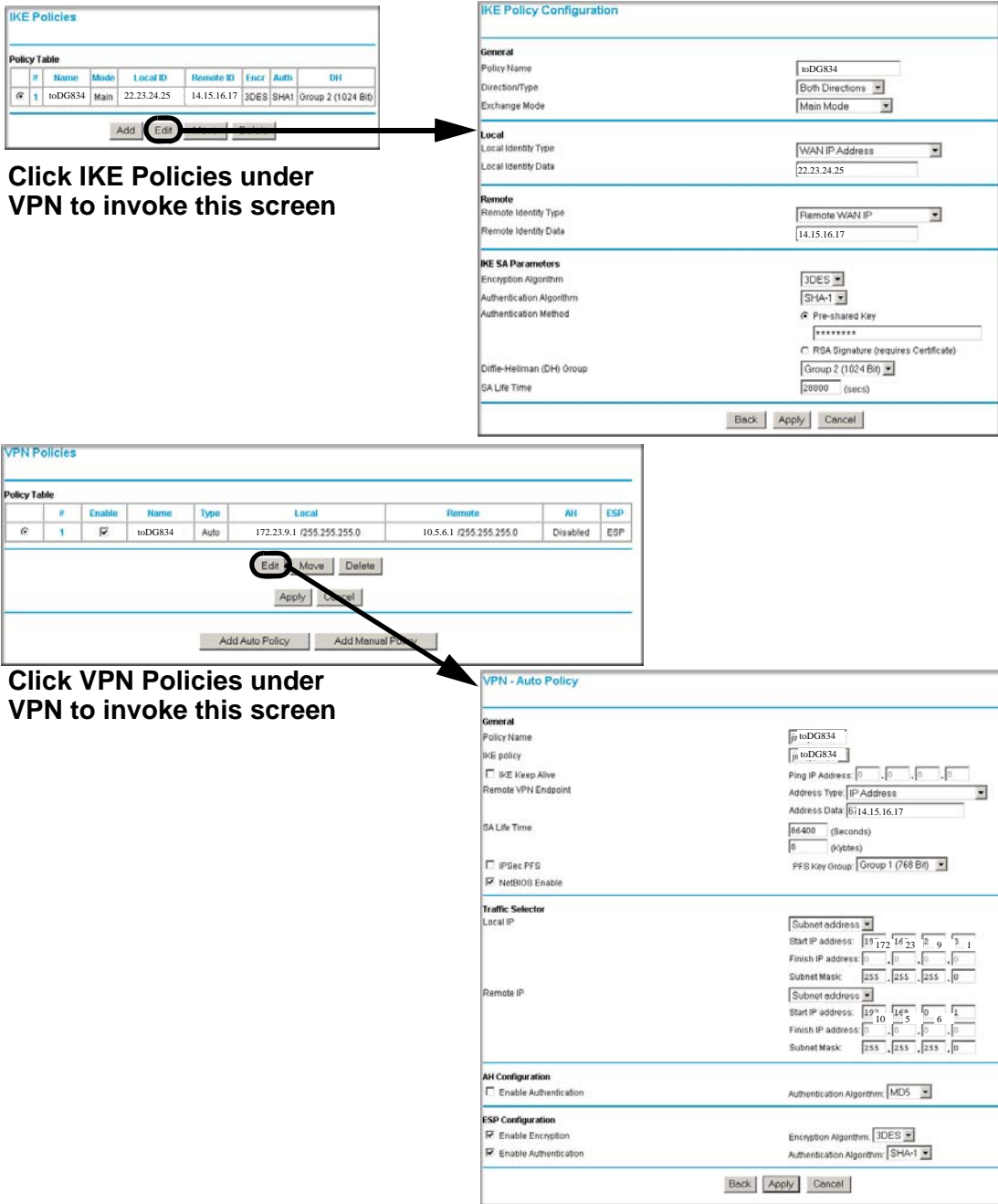
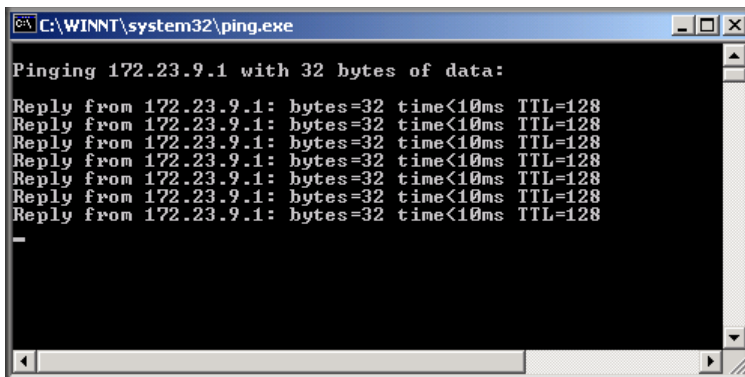


Figure B-3

3. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834 v3.
 - a. Open the command prompt (Start -> Run -> cmd)
 - b. ping 172.23.9.1




```
C:\WINNT\system32\ping.exe

Pinging 172.23.9.1 with 32 bytes of data:

Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
```

Figure B-4

	Note: The pings may fail the first time. If this happens, try the pings a second time.
-----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------

DG834 v3 with FQDN to FVL328

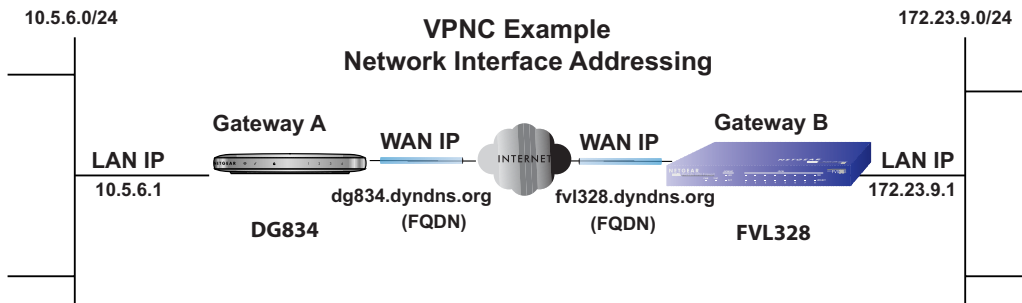
This appendix is a case study on how to configure a VPN tunnel from a NETGEAR DG834 v3 to a FVL328 using a Fully Qualified Domain Name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>).

Configuration Profile

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

Table B-1. Profile Summary

VPN Consortium Scenario:	Scenario 1
Type of VPN	LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)
Security Scheme:	IKE with Preshared Secret/Key (not Certificate-based)
IP Addressing:	
NETGEAR-Gateway A	Fully Qualified Domain Name (FQDN)
NETGEAR-Gateway B	FDQN

**Figure B-5**

Note: Product updates are available on the NETGEAR, Inc. web site at <http://kbserver.netgear.com/DG834 v3.asp>.

The Use of a Fully Qualified Domain Name (FQDN)

Many ISPs (Internet Service Providers) provide connectivity to their customers using dynamic instead of static IP addressing. This means that a user's IP address does not remain constant over time which presents a challenge for gateways attempting to establish VPN connectivity.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host or domain name. It provides a central public database where information (such as email addresses, host names and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a 3rd party service in lieu of a permanent and unchanging IP address to establish bi-directional VPN connectivity.

To use DDNS, you must register with a DDNS service provider. Example DDNS Service Providers include:

- DynDNS: www.dyndns.org
- TZO.com: netgear.tzo.com
- ngDDNS: ngddns.iego.net

In this example, Gateway A is configured using an example FQDN provided by a DDNS Service provider. In this case we established the hostname **dg834.dyndns.org** for gateway A using the DynDNS service. Gateway B will use the DDNS Service Provider when establishing a VPN tunnel.

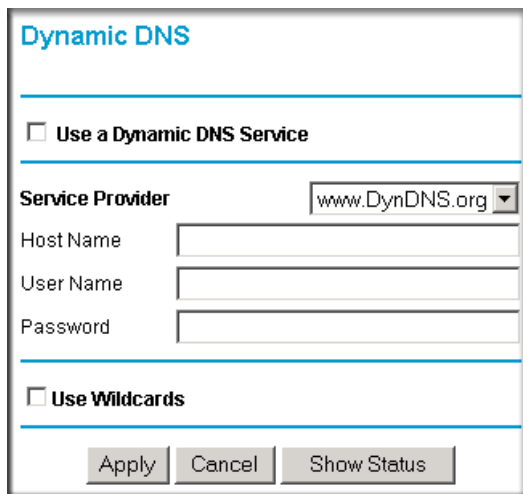
In order to establish VPN connectivity Gateway A must be configured to use Dynamic DNS, and Gateway B must be configured to use a DNS hostname to find Gateway A provided by a DDNS Service Provider. Again, the following step-by-step procedures assume that you have already registered with a DDNS Service Provider and have the configuration information necessary to set up the gateways.

Step-By-Step Configuration

1. Log in to the DG834 v3 labeled Gateway A as in the illustration.

Out of the box, the DG834 v3 is set for its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. Click on the Dynamic DNS link on the left side of the Settings management GUI. This will take you to the Dynamic DNS Menu.
3. On the DG834 v3, configure the Dynamic DNS settings.
 - a. Browse to the Dynamic DNS Setup Screen (see [Figure B-6](#)) in the Advanced menu.



Dynamic DNS

Use a Dynamic DNS Service

Service Provider:

Host Name:

User Name:

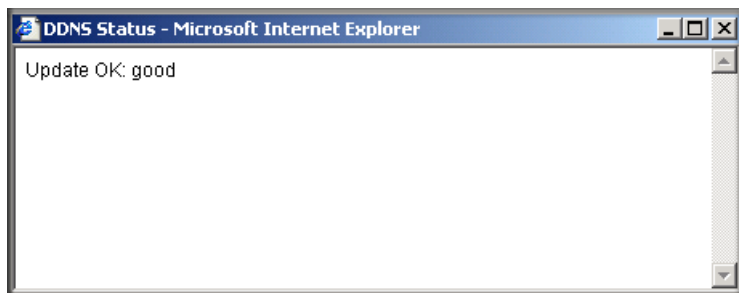
Password:

Use Wildcards

Apply Cancel Show Status

Figure B-6

- b. Configure this screen with appropriate account and hostname settings and then click **Apply**.
 - Check the box **Use a Dynamic DNS Service**.
 - Host Name = dg834.dyndns.org
 - User Name = <user's account username>
 - Password = <user's account password>
- c. Click **Show Status**. The resulting screen should show Update OK: good (see [Figure B-7](#)).

**Figure B-7**

4. On the FVL328, configure the Dynamic DNS settings. Assume a properly configured DynDNS account.

- a. Browse to the Dynamic DNS Setup Screen (see [Figure B-8](#)) in the Advanced menu.

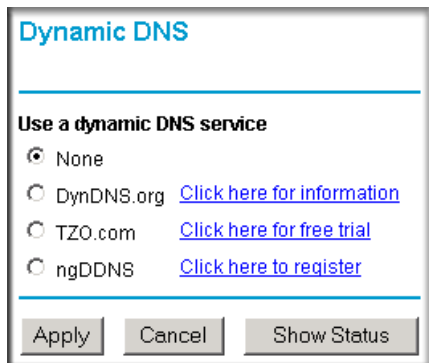


Figure B-8

- b. Select the DynDNS.org radio button (see [Figure B-8](#)), configure with appropriate account and hostname settings (see [Figure B-9](#)), and then click **Apply**.
- Host and Domain Name = fv1328.dyndns.org
 - User Name = <user's account username>

- Password = <user's account password>

Dynamic DNS

Use a dynamic DNS service

None

DynDNS.org [Click here for information](#)

TZO.com [Click here for free trial](#)

ngDDNS [Click here to register](#)

DynDNS

Host and Domain Name

example: yourname.dyndns.org

User Name

Password

Use wildcards

Figure B-9

- c. Click **Show Status**. The resulting screen should show Update OK: good (see [Figure B-10](#)).

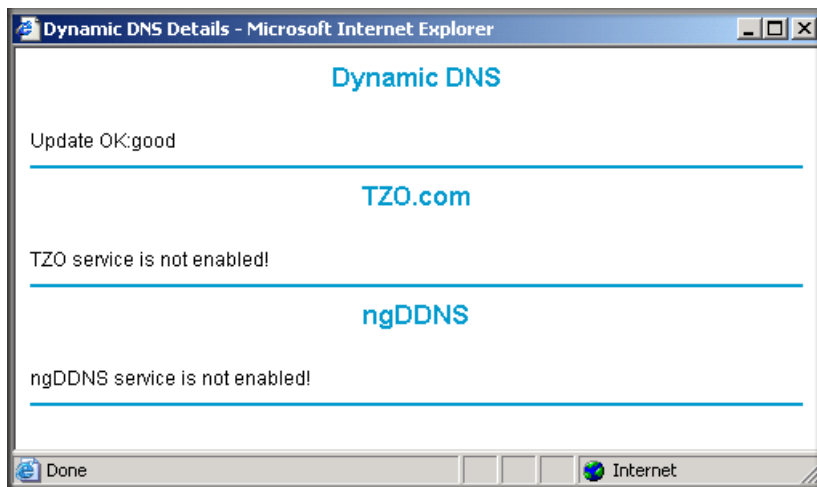


Figure B-10

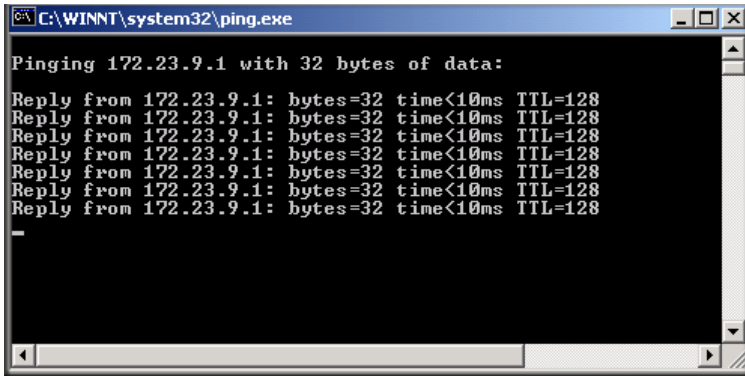
5. Configure the DG834 v3 as in the Gateway-to-Gateway procedures using the VPN Wizard (see [“How to Set Up a Gateway-to-Gateway VPN Configuration”](#) on page 6-20), being certain to use appropriate network addresses for the environment.

The LAN Addresses used in this example are as follows:

Device	LAN IP Address	LAN Subnet Address
DG834 v3	10.5.6.1	255.255.255.0
FVL328	172.23.9.1	255.255.255.0

- a. In Step 1, enter **toFVL328** for the Connection Name.
 - b. In Step 2, enter **fv1328.dyndns.org** for the remote WAN's IP address.
 - a. In Step 3, enter the following:
 - IP Address = **172.23.9.1**
 - Subnet Mask = **255.255.255.0**
6. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see [“How to Set Up a Gateway-to-Gateway VPN Configuration”](#) on page 6-20), being certain to use appropriate network addresses for the environment.

- a. In Step 1, enter **toDG834** for the Connection Name.
 - b. In Step 2, enter **dg834.dyndns.org** for the remote WAN's IP address.
 - c. In Step 3, enter the following:
 - IP Address = **10.5.6.1**
 - Subnet Mask = **255.255.255.0**
7. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834 v3.
- a. Open the command prompt (Start -> Run -> cmd)
 - b. ping 172.23.9.1



```
C:\WINNT\system32\ping.exe
Pinging 172.23.9.1 with 32 bytes of data:
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
-
```

Figure B-11



Note: The pings may fail the first time. If this happens, try the pings a second time.

Configuration Summary (Telecommuter Example)

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Assure that there are no firewall restrictions.

Table B-1. Configuration summary (telecommuter example)

VPN Consortium Scenario:	Scenario 1
Type of VPN:	PC/client-to-gateway, with client behind NAT router
Security Scheme:	IKE with Preshared Secret/Key (not Certificate-based)
IP Addressing:	
Gateway	Fully Qualified Domain Name (FQDN)
Client	Dynamic

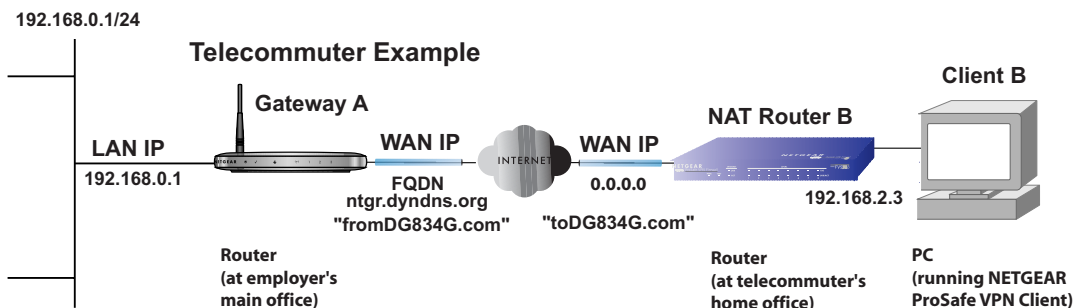


Figure B-12

Setting Up the Client-to-Gateway VPN Configuration (Telecommuter Example)

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway involves the following two steps:

- [Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office.](#)
- [Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office](#) configures the NETGEAR ProSafe VPN Client endpoint.

Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office

Follow this procedure to configure a client-to-gateway VPN tunnel by filling out the VPN Auto Policy screen.

1. Log in to the VPN router at its LAN address of <http://192.168.0.1> with its default user name of **admin** and password of **password**. Click the VPN Policies link in the main menu to display the VPN Policies screen. Click **Add Auto Policy** to proceed and enter the information.

VPN - Auto Policy

General

Policy Name: fromDG834G

Remote VPN Endpoint Address Type: Dynamic IP address

Address Data: n/a

NetBIOS Enable

IKE Keep Alive Ping IP Address: 192 . 168 . 2 . 3

Local LAN

IP Address Subnet address

Single/Start address: 192 . 168 . 0 . 1

Finish address:

Subnet Mask: 255 . 255 . 255 . 0

Remote LAN

IP Address Single address

Single/Start IP address: 192 . 168 . 2 . 3

Finish IP address:

Subnet Mask:

IKE

Direction: Responder only

Exchange Mode: Main Mode

Diffie-Hellman (DH) Group: Auto

Local Identity Type: Fully Qualified Domain Name

Data: fromDG834G.com

Remote Identity Type: Fully Qualified Domain Name

Data: toDG834G.com

Parameters

Encryption Algorithm: 3DES

Authentication Algorithm: Auto

Pre-shared Key: 12345678

SA Life Time: 3600 (seconds)

Enable PFS (Perfect Forward Security)

Buttons: Back, Apply, Cancel

Annotations:

- fromDG834G (in the example) Dynamic IP address
- IKE Keep Alive is optional; must match Remote LAN IP Address when enabled (remote PC must respond to pings)
- Subnet address 192.168.0.1 (in this example) 255.255.255.0
- Single address 192.168.2.3 (in this example) (Remote NAT router must have Address Reservation set and VPN Passthrough enabled)
- Main Mode
- Fully Qualified Domain Name fromDG834G.com (in this example)
- Fully Qualified Domain Name toDG834G.com (in this example)
- 3DES 12345678 (in this example) 3600

Figure B-13

2. Click **Apply** when done to get the **VPN Policies** screen.

VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	fromDG834G	Auto	192.168.0.1 / 255.255.255.0	192.168.2.3	3DES

Edit Delete

Apply Cancel

Add Auto Policy Add Manual Policy

Figure B-14

To view or modify the tunnel settings, select the radio button next to the tunnel entry and click **Edit**.

Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office


This procedure describes how to configure the DG834 ADSL Modem Router. We will assume the PC running the client has a dynamically assigned IP address.


The PC must have a VPN client program installed that supports IPSec (in this case study, the NETGEAR VPN ProSafe Client is used). Go to the NETGEAR website (<http://www.netgear.com>) and select VPN01L_VPN05L in the **Product Quick Find** drop-down menu for information on how to purchase the NETGEAR ProSafe VPN Client.




Note: Before installing the DG834 ADSL Modem Router software, be sure to turn off any virus protection or firewall software you may be running on your PC.

1. Install the NETGEAR ProSafe VPN Client on the remote PC and reboot.
 - a. You may need to insert your Windows CD to complete the installation.
 - b. If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating “The **NETGEAR ProSafe VPN** Component requires at least one dial-up adapter be installed.” You can disregard this message.

- c. Install the **IPSec Component**. You may have the option to install either the **VPN Adapter** or the **IPSec Component** or both. The **VPN Adapter** is not necessary.
 - d. The system should show the **ProSafe** icon () in the system tray after rebooting.
 - e. Double-click the system tray icon to open the **Security Policy Editor**.
2. Add a new connection.
 - a. Run the **NETGEAR ProSafe Security Policy Editor** program and create a **VPN Connection**.
 - b. From the **Edit** menu of the **Security Policy Editor**, click **Add**, then **Connection**. A **New Connection** listing appears in the list of policies. Rename the **New Connection** so that it matches the **Connection Name** you entered in the **VPN Settings** of the DG834 v3 on Gateway A.

 **Note:** In this example, the **Connection Name** used on the client side of the VPN tunnel is **toDG834G** and it does not have to match the **VPN_client Connection Name** used on the gateway side of the VPN tunnel (see [Figure B-16](#)) because Connection Names are arbitrary to how the VPN tunnel functions.

 **Tip:** Choose Connection Names that make sense to the people using and administrating the VPN.

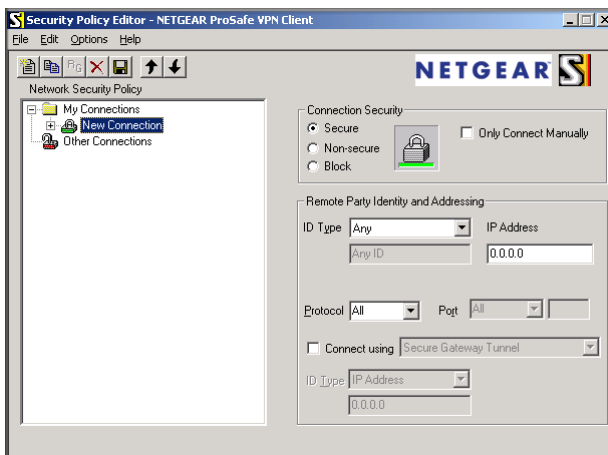


Figure B-15

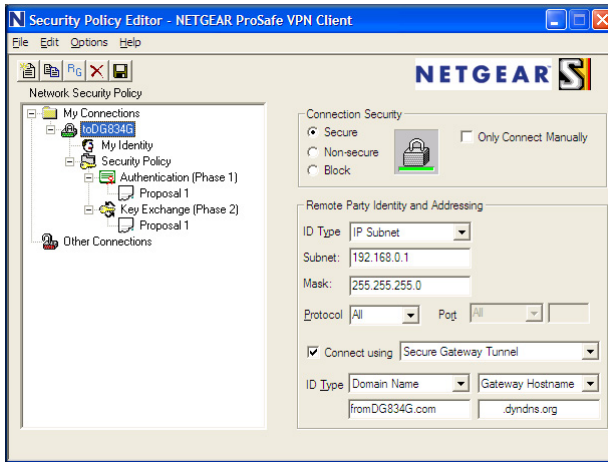


Figure B-16

- c. Select **Secure** in the **Connection Security** check box.
 - d. Select **IP Subnet** in the **ID Type** menu.
 - e. In this example, type **192.168.0.1** in the Subnet field as the network address of the DG834 v3.
 - f. Enter **255.255.255.0** in the Mask field as the **LAN Subnet Mask** of the DG834 v3.
 - g. Select **All** in the **Protocol** menu to allow all traffic through the VPN tunnel.
 - h. Select the **Connect using Secure Gateway Tunnel** check box.
 - i. Select **Domain Name** in the **ID Type** menu below the check box and enter **fromDG834G.com** (in this example).
 - j. Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).
 - k. The resulting Connection Settings are shown in [Figure B-16](#).
3. Configure the **Security Policy** in the DG834 ADSL Modem Router software.
 - a. In the **Network Security Policy** list, expand the new connection by double clicking its name or clicking on the “+” symbol. **My Identity** and **Security Policy** subheadings appear below the connection name.

- b. Click on the **Security Policy** subheading to show the **Security Policy** menu.

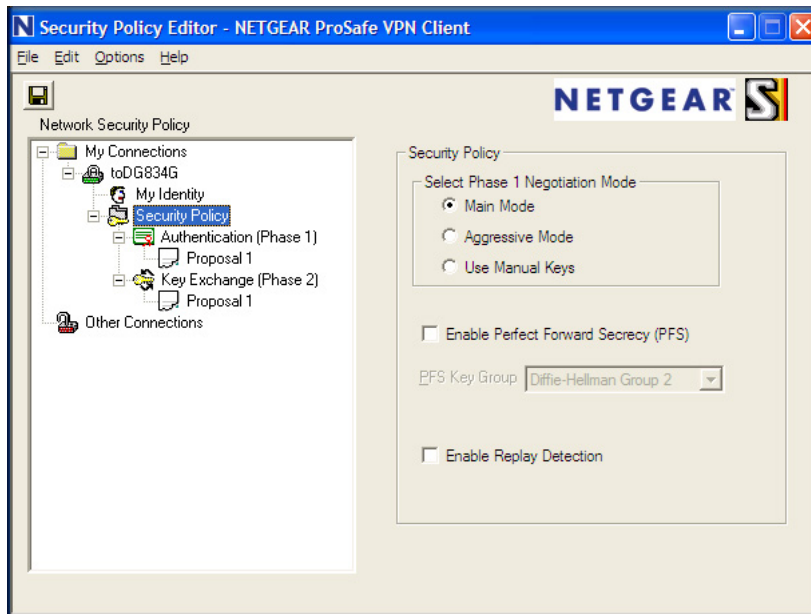


Figure B-17

- c. Select the **Main Mode** in the **Select Phase 1 Negotiation Mode** check box.
4. Configure the **VPN Client Identity**.

In this step, you will provide information about the remote VPN client PC. You will need to provide the Pre-Shared Key that you configured in the DG834 v3 and either a fixed IP address or a “fixed virtual” IP address of the VPN client PC.

- a. In the **Network Security Policy** list on the left side of the **Security Policy Editor** window, click **My Identity**.

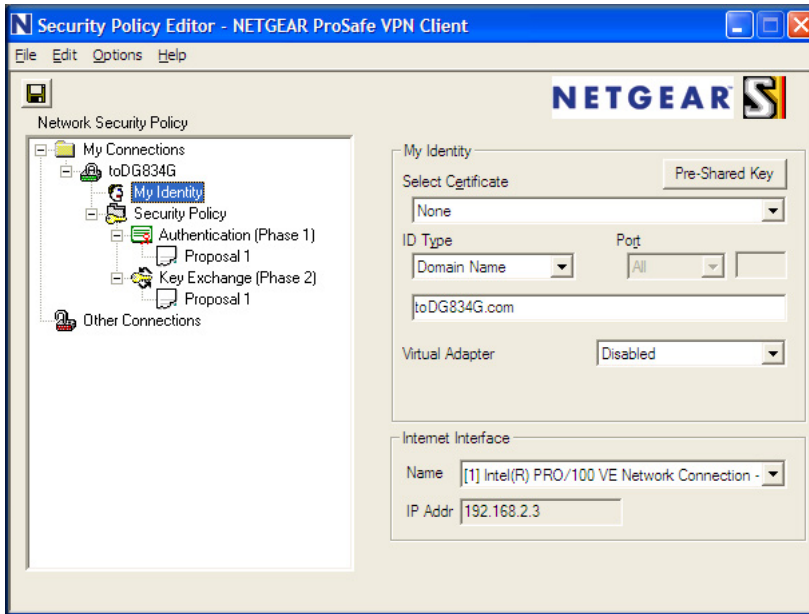


Figure B-18

- b. Choose **None** in the **Select Certificate** menu.
- c. Select **Domain Name** in the **ID Type** menu and enter **toDG834G.com** (in this example) in the box below it. Choose **Disabled** in the **Virtual Adapter** menu.
- d. In the **Internet Interface** box, select **Intel PRO/100VE Network Connection** (in this example, your Ethernet adapter may be different) in the **Name** menu and enter **192.168.2.3** (in this example) in the **IP Addr** box.

- e. Click the **Pre-Shared Key** button. In the **Pre-Shared Key** dialog box, click the **Enter Key** button. Enter the DG834 v3's **Pre-Shared Key** and click **OK**. In this example, **12345678** is entered. This field is case sensitive.

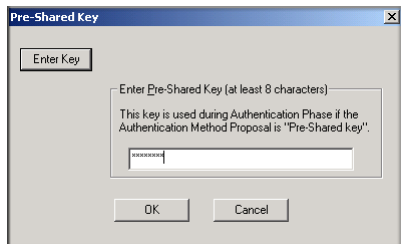


Figure B-19

5. Configure the **VPN Client Authentication Proposal**.

In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the VPN router configuration.

- a. In the **Network Security Policy** list on the left side of the **Security Policy Editor** window, expand the **Security Policy** heading by double clicking its name or clicking on the “+” symbol.

- b. Expand the **Authentication** subheading by double clicking its name or clicking on the “+” symbol. Then select **Proposal 1** below **Authentication**.

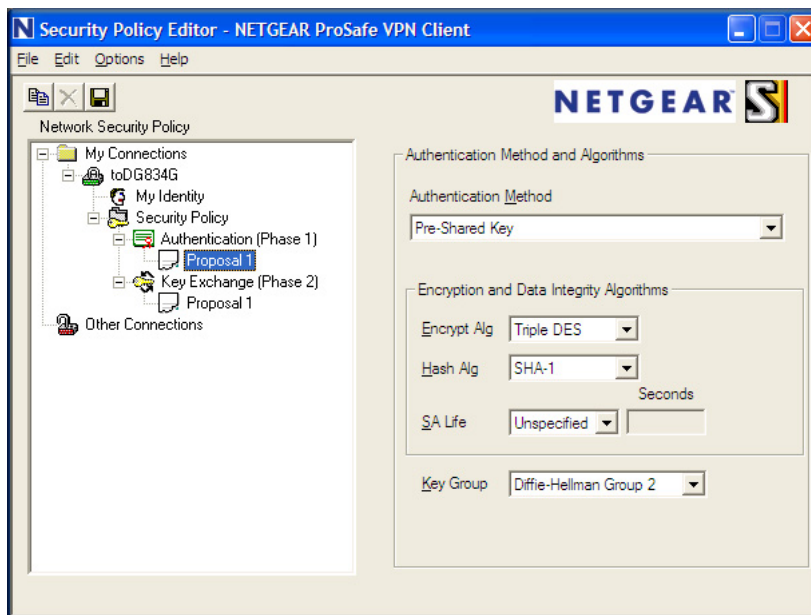


Figure B-20

- c. In the **Authentication Method** menu, select **Pre-Shared key**.
 - d. In the **Encrypt Alg** menu, select the type of encryption. In this example, use **Triple DES**.
 - e. In the **Hash Alg** menu, select **SHA-1**.
 - f. In the **SA Life** menu, select **Unspecified**.
 - g. In the **Key Group** menu, select **Diffie-Hellman Group 2**.
6. Configure the **VPN Client Key Exchange Proposal**.

In this step, you will provide the type of encryption (**DES** or **3DES**) to be used for this connection. This selection must match your selection in the VPN router configuration.

- a. Expand the **Key Exchange** subheading by double clicking its name or clicking on the “+” symbol. Then select **Proposal 1** below **Key Exchange**.

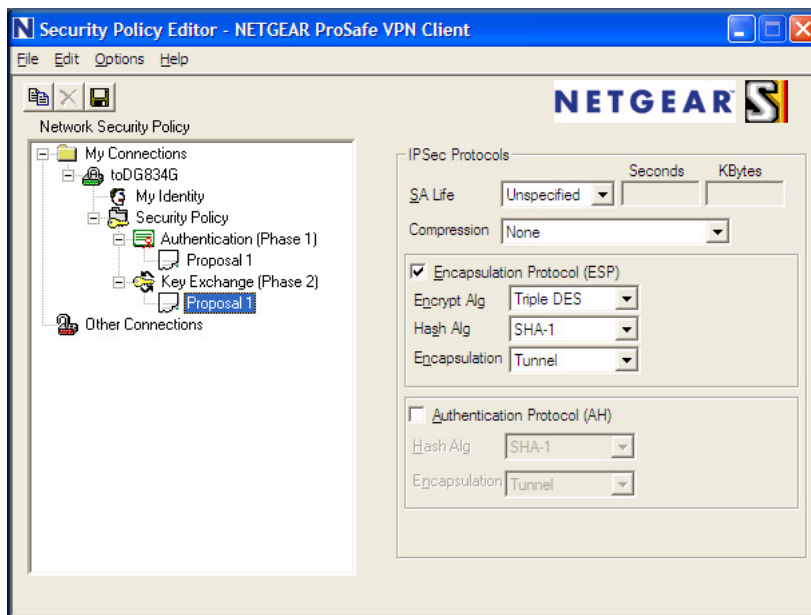


Figure B-21

- b. In the **SA Life** menu, select **Unspecified**.
 - c. In the **Compression** menu, select **None**.
 - d. Check the **Encapsulation Protocol (ESP)** checkbox.
 - e. In the **Encrypt Alg** menu, select the type of encryption. In this example, use **Triple DES**.
 - f. In the **Hash Alg** menu, select **SHA-1**.
 - g. In the **Encapsulation** menu, select **Tunnel**.
 - h. Leave the **Authentication Protocol (AH)** checkbox unchecked.
7. Save the VPN Client settings.

From the **File** menu at the top of the **Security Policy Editor** window, select **Save**.

After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router's LAN.

8. Check the VPN Connection.

To check the **VPN Connection**, you can initiate a request from the remote PC to the VPN router's network by using the **Connect** option in the DG834 ADSL Modem Router menu bar (see [Figure B-22](#)). Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

- a. Right-click the system tray icon to open the popup menu.
- b. Select **Connect** to open the **My Connections** list.
- c. Choose **toDG834G**.

The DG834 ADSL Modem Router will report the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.

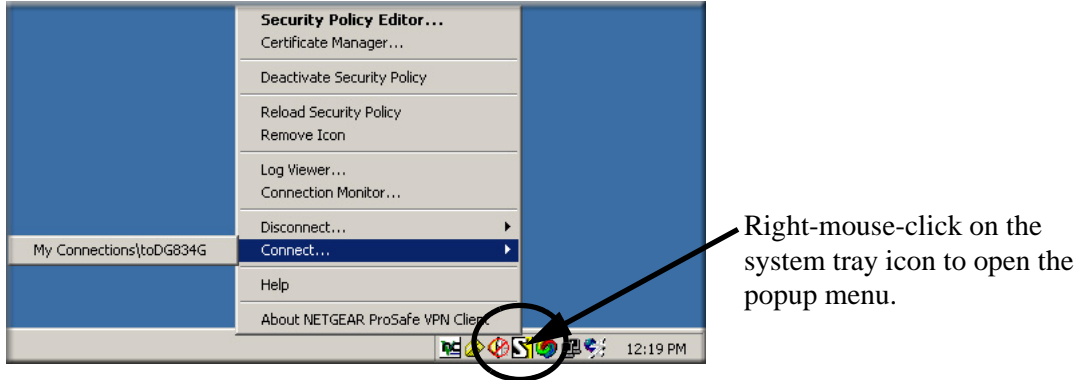


Figure B-22

To perform a ping test using our example, start from the remote PC:

- a. Establish an Internet connection from the PC.
- b. On the **Windows** taskbar, click the Start **button**, and then click **Run**.

- c. Type **ping -t 192.168.0.1**, and then click **OK**.

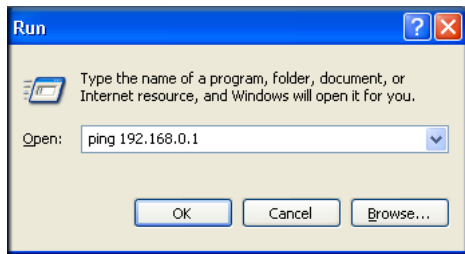


Figure B-23

This will cause a continuous ping to be sent to the VPN router. After between several seconds and two minutes, the ping response should change from **timed out** to **reply**.

```
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
```

Figure B-24

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the VPN router. After a short wait, you should see the login screen of the VPN router (unless another PC already has the VPN router management interface open).



Note: You can use the VPN router diagnostic utilities to test the VPN connection from the VPN router to the client PC. Run ping tests from the **Diagnostics** link of the VPN router main menu.

Monitoring the VPN Tunnel (Telecommuter Example)

Viewing the PC Client's Connection Monitor and Log Viewer

To view information on the progress and status of the VPN client connection, open the DG834 ADSL Modem Router **Log Viewer**.

1. To launch this function, click on the Windows **Start** button, then select **Programs**, then DG834 ADSL Modem Router, then **Log Viewer**.



Note: Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

2. The **Connection Monitor** screen is shown below:

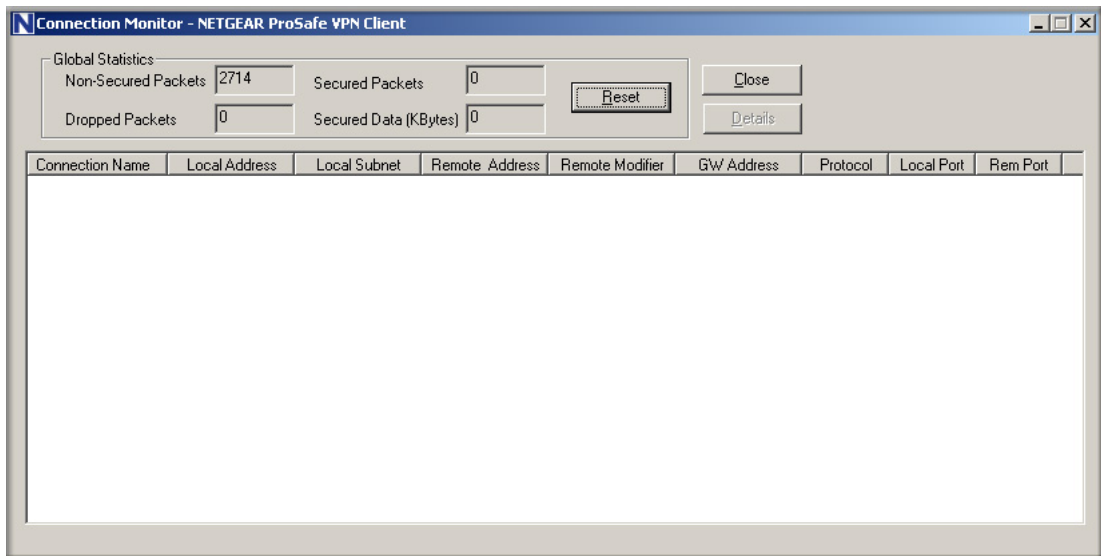


Figure B-25

While the connection is being established, the **Connection Name** field in this menu will show **SA** before the name of the connection. When the connection is successful, the **SA** will change to the yellow key symbol.



Note: While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you will need to close the VPN connection in order to have normal Internet access.

Viewing the VPN Router's VPN Status and Log Information

To view information on the status of the VPN client connection, open the VPN router's VPN Status screen by following the steps below:

1. To view this screen, click the **Router Status** link of the VPN router's main menu, then click the **VPN Status** button. The **VPN Status/Log** screen for a connection is shown below:

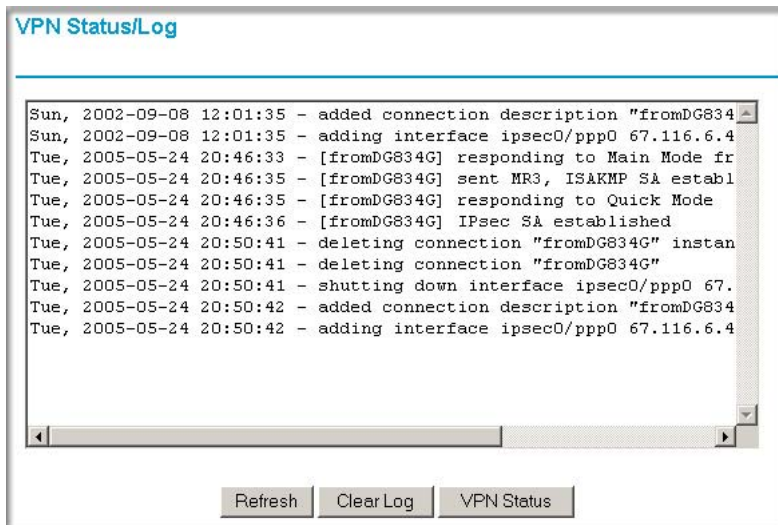
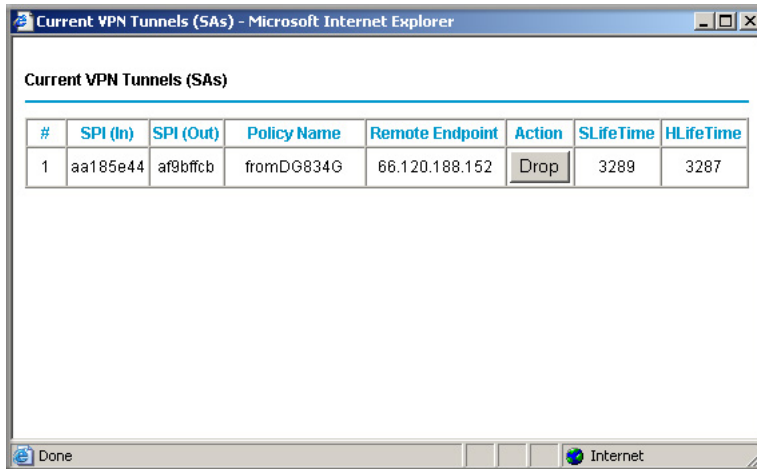


Figure B-26

- To view the VPN tunnels status, click the **VPN Status** link on the right side of the main menu.



#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	aa185e44	af9bffc8	fromDG834G	66.120.188.152	Drop	3289	3287

Figure B-27

Current VPN Tunnels (SAs) screen

Appendix C

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

