ADSL2+ Modem Wireless Router DG834G Reference Manual

NETGEAR®

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

Trademarks

NETGEAR and the NETGEAR logo are trademarks 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.

FCC Statement

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 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

The radio module has been evaluated under FCC Bulletin OET 65C (01-01) and found to be compliant to the requirements as set forth in CFR 47 Sections, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. This model meets the applicable government requirements for exposure to radio frequency waves.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. For product available in the USA market, only channels 1~11 can be operated. Selection of other channels is not possible

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.

Èesky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento 54 Mbps ADSL2+ Modem Wireless Router Model DG834G je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr 54 Mbps ADSL2+ Modem Wireless Router Model DG834G overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät 54 Mbps ADSL2+ Modem Wireless Router Model DG834G in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme 54 Mbps ADSL2+ Modem Wireless Router Model DG834G vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this 54 Mbps ADSL2+ Modem Wireless Router Model DG834G is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente NETGEAR, Inc. declara que el 54 Mbps ADSL2+ Modem Wireless Router Model DG834G cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR, Inc. ΔΗΛΩΝΕΙ ΟΤΙ 54 Mbps ADSL2+ Modem Wireless Router Model DG834G ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente NETGEAR, Inc. déclare que l'appareil 54 Mbps ADSL2+ Modem Wireless Router Model DG834G est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente NETGEAR, Inc. dichiara che questo 54 Mbps ADSL2+ Modem Wireless Router Model DG834G è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarç, ka 54 Mbps ADSL2+ Modem Wireless Router Model DG834G atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis 54 Mbps ADSL2+ Modem Wireless Router Model DG834G atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel 54 Mbps ADSL2+ Modem Wireless Router Model DG834G in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, NETGEAR, Inc., jiddikjara li dan 54 Mbps ADSL2+ Modem Wireless Router Model DG834G jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a 54 Mbps ADSL2+ Modem Wireless Router Model DG834G megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oœwiadcza, ¿e 54 Mbps ADSL2+ Modem Wireless Router Model DG834G jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este 54 Mbps ADSL2+ Modem Wireless Router Model DG834G está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta 54 Mbps ADSL2+ Modem Wireless Router Model DG834G v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že 54 Mbps ADSL2+ Modem Wireless Router Model DG834G spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että 54 Mbps ADSL2+ Modem Wireless Router Model DG834G tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the DG834G v4 product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das 54 Mbps ADSL2+ Modem Wireless Router Model DG834G gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the 54 Mbps ADSL2+ Modem Wireless Router Model DG834G has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your 54 Mbps ADSL2+ Modem Wireless Router Model DG834G.

World Wide Web

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

Product and Publication Details

Model Number:	DG834G v4
Publication Date:	September 2007
Product Family:	Modem Router
Product Name:	54 Mbps ADSL2+ Modem Wireless Router Model DG834G
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10269-01
Publication Version Number:	2.0

Contents

ADSL2+ Modem Wireless Router DG834G Reference Manual

v2.0, September 2007

Chapter 4
Managing Your Network

Chapter 5
Advanced Configuration

4

Appendix C
Related Documents

v2.0, September 2007

About This Manual

The *NETGEAR® ADSL2+ Modem Wireless Router DG834G Reference Manual* describes how to install, configure ,and troubleshoot the 54 Mbps ADSL2+ Modem Wireless Router Model DG834G. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats, and Scope

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

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

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
italic	URL links

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

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

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

Warning: Ignoring this type of note might result in a malfunction or damage to the equipment.

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

Product Version	54 Mbps ADSL2+ Modem Wireless Router Model DG834G
Manual Publication Date	September 2007

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

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

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print this Manual

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

- **Printing a page in the HTML view**.

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

- **Printing a chapter**.

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

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

– Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe website at *http://www.adobe.com*.
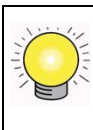
– Click the print icon in the upper left of the window.

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

- **Printing the full manual**.

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

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

  – Click the print icon in the upper left of the window.
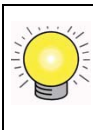
> **Tip:** If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 1
Configuring Your Internet Connection

This chapter describes how to configure your ADSL2+ Modem Wireless Router Internet connection. When you perform the initial configuration of your modem router using the *DG834G ADSL2+ Modem Wireless Router Resource CD* as described in the *NETGEAR Router Setup Manual,* these settings are configured automatically for you. This chapter provides further details about these settings, as well as instructions on how to log in to the modem router for further configuration.

> **Note:** NETGEAR recommends using the Smart Wizard on the *DG834G ADSL2+ Modem Wireless Router Resource CD* for initial configuration, as described in the *NETGEAR Router Setup Manual*.

This chapter includes:

- "Using the Setup Manual "
- "What You Need Before You Begin"
- "Logging In to the Modem Router"
- "Understanding the Basic Settings Screen"
- "ADSL Settings"

Using the Setup Manual

For first-time installation of your modem router, refer to the *NETGEAR Router Setup Manual*. The Setup Manual explains how to launch the NETGEAR Smart Wizard on the *DG834G ADSL2+ Modem Wireless Router Resource CD* to step you through the procedure to connect your router, modem, and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network. After initial configuration using the Setup Manual, you can use the information in this Reference Manual to configure additional features of your wireless router.

For installation instructions in a language other than English, see the language options on the *DG834G ADSL2+ Modem Wireless Router Resource CD.*

What You Need Before You Begin

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

• Active Internet service provided by an ADSL account.

• The Internet Service Provider (ISP) configuration information for your ADSL account.

– ISP login name and password

– ISP Domain Name Server (DNS) addresses

– Fixed or static IP address

– Host and domain names

• Depending on how your ISP set up your Internet account, you need to know one or more of these settings:

– Virtual path identifier (VPI) and Virtual channel identifier (VCI) parameters

– Multiplexing method

– Host and domain names

• ASDL microfilters as explained in the *NETGEAR Router Setup Manual*.

• Your computer must be set up to use DHCP to get its TCP/IP configuration from the modem router. This is usually the case. For help with DHCP, see the documentation that came with your computer, or see the link to the online document in "Preparing a Computer for Network Access" in Appendix C.

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

Logging In to the Modem Router

You can log in to the modem router to view or change its settings.

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

To log in to the modem router:

1. Type **http://routerlogin.net** or **http://192.168.0.1** in the address field of an Internet browser.

Figure 1-1

This login window opens:

Figure 1-2

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

3. Select Setup Wizard to go to the Setup Wizard screen:

Figure 1-3

v2.0, September 2007
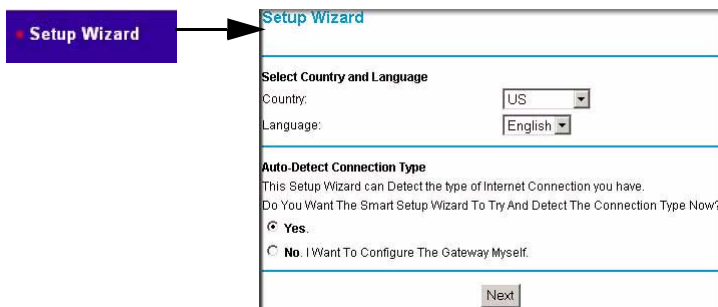
This screen includes the following:

- **Country**. It is important to specify the location where the modem router will operate so that the Internet connection will work correctly.

- **Language**. You can select a language from the drop-down list.

- **Auto-Detect Connection Type**. If you want to change the settings for the Internet connection, select **Yes** or **No**, and then click **Next**.

  - **Yes**. Let the modem router Setup Wizard auto-detect the type of Internet connection that you have and configure it. See "Auto-Detecting Your Internet Connection".

  - **No, I want to Configure the Router Myself**. Enter your Internet settings manually in the Basic Settings screen. See "Understanding the Basic Settings Screen" on page 1-7.

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

- **Test**. To test your Internet connection, click **Test**. If the NETGEAR website does not appear within 1 minute, see Chapter 7, "Troubleshooting".

Auto-Detecting Your Internet Connection

The Smart Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

> **→** **Note:** The wizard cannot detect a PPTP connection with your ISP. If your ISP uses this protocol, then you must configure your connection manually (see "Understanding the Basic Settings Screen" on page 1-7).

To use the Smart Setup Wizard to assist with configuration or to view the Internet connection settings:

1. From the Setup Wizard screen, select **Yes** for the Auto-Detect Connection Type, and then click **Next** to proceed.

The Setup Wizard detects your ISP configuration. Depending on the type of connection, you are prompted to enter your ISP settings, as shown in the following table.

Table 1-1. Auto-Detected Internet Connection Types

Connection Type	ISP Information
PPP over Ethernet (PPPoE) PPP over ATM (PPPoA)	Enter the login user name and password. These fields are case-sensitive.
Dynamic IP Account Setup	No entries needed.
IP over ATM Classical IP assignment (RFC1577)	• Enter the assigned IP address, subnet mask, and the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. • DNS servers are required to perform the function of translating an Internet name such as *www.netgear.com* to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here.
Fixed IP (Static) Account Setup	1. If required, enter the account name and domain name from your ISP. 2. Select **Use Static IP Address** or **Use IP Over ATM** (IPoA — RFC1483 Routed) according to the information from your ISP. If you select IPoA, the router will detect the gateway IP address, but you still need to provide the router IP address. 3. Enter your assigned IP address, subnet mask, and the IP address of your ISP's gateway modem router. This information should have been provided to you by your ISP. 4. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. DNS servers are required to perform the function of translating an Internet name such as *www.netgear.com* to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here.

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

3. Click **Test** to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 7, "Troubleshooting".

Viewing or Manually Configuring Your ISP Settings

NETGEAR recommends that you specify your country and language before you configure the settings on the Basic Settings screen. See "Logging In to the Modem Router" on page 1-2. You must install the ADSL filters and connect the modem router to the ADSL line as described in the *NETGEAR Router Setup Manual* before you configure the settings in the Basic Settings screen.

To view or configure the basic settings:

1. Log in to the modem router as described in "Logging In to the Modem Router".

2. Select Basic Settings to display the Basic Settings screen.

   The Basic Settings screen is explained in "Understanding the Basic Settings Screen" on page 1-7.

3. Select **Yes** or **No** depending on whether your ISP requires a login. This selection changes the fields available on the Basic Settings screen.

   • **Yes**. If your ISP requires a login, select the encapsulation method. Enter the login name. If you want to change the login time-out, enter a new value in minutes.

   • **No**. If your ISP does not require a login, enter the account name, if required, and the domain name, if required.

4. Enter the settings for the IP address and DNS server.

   The default ADSL settings usually work fine. If you have problems with your connection, check the ADSL settings. See "ADSL Settings" for more details.

5. If no login is required, you can specify the MAC Address setting.

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

7. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, "Troubleshooting".

> **Note:** When your Internet connection is working you will no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in.

Understanding the Basic Settings Screen

The fields on the Basic Settings screen depend on whether or not your Internet connection requires a login.

ISP *does not* require login   **ISP *does* require login**

Figure 1-4

The following table explains the fields in the Basic Settings screen. Note that the group of fields included in this screen depends on whether or not a login is required.

Table 1-2.   Basic Settings screen fields

Settings		Description
Does Your ISP Require a Login?		• Yes • No
These fields appear only if no login is required.	Account Name (If required)	Enter the account name provided by your ISP. This might also be called the host name.
	Domain Name (If required)	Enter the domain name provided by your ISP.
These fields appear only if your ISP requires a login.	Encapsulation	• PPPoE • PPPoA • PPTP
	Login	The login name provided by your ISP. This is often an e-mail address.
	Idle Timeout (In minutes)	If you want to change the login time-out, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out.
Internet IP Address		• **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses. • **Use Static IP Address**. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP's modem router to which your modem router will connect. • **Use IP Over ATM (IFoA)**. Your ISP uses Classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned.
Domain Name Server (DNS) Address		The DNS server is used to look up site addresses based on their names. • **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address. • **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

Table 1-2.   Basic Settings screen fields (continued)

Settings		Description
NAT (Net Address Translation)		NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices. • **Enable**. Usually NAT is enabled. • **Disable**. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure that you do not require it. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses that the DG834G v4 uses. Classical routing should be selected only by experienced users[*] • **Disable Firewall**. This disables the firewall in addition to disabling NAT. With the firewall disabled, the protections usually provided to your network are disabled.
This field appears only if no login is required.	Router MAC Address	The Ethernet MAC address that will be used by the modem router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your modem router to masquerade as that computer by "cloning" its MAC address. • **Use Default Address**. Use the default MAC address. • **Use Computer MAC Address**. The modem router will capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. • **Use This MAC Address**. Enter the MAC address that you want to use.

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

ADSL Settings

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

The default ADSL settings of your modem router work fine for most ISPs. However, some ISPs use a specific multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI).

→ **Note:** You must use the Setup Wizard to select the correct country for the default ADSL settings to work.

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

1. From the main menu, select **ADSL Settings**.

2. In the **Multiplexing Method** drop-down list, select **LLC-based** or **VC-based**.

3. Type a number between 0 and 255 for the VPI. The default is 8.

4. Type a number between 32 and 65535 for the VCI. The default is 35.

5. Click **Apply**.

How the Internet Connection Works

Your modem router is now configured to provide Internet access for your network. Your modem router automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as dial-up networking or Enternet to connect, log in, or disconnect. The modem router performs these functions automatically as needed.

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

Chapter 2
Wireless Configuration

This chapter describes how to configure the wireless features of your ADSL2+ Modem Wireless Router. In planning your wireless network, consider the level of security required. You should also select the physical placement of your modem router to maximize the network speed.

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

For proper compliance and compatibility between similar products in your area, you must set the operating channel and region correctly.

Set up wireless features for the modem router in this order:

1. Connect the modem router, and get the Internet connection working, as described in Chapter 1, "Configuring Your Internet Connection". The modem router should work with an Ethernet LAN connection before you set up the wireless features.

2. Plan the location for the modem router based on considerations in "Wireless Placement and Range Guidelines".

3. Enter the wireless settings, and verify wireless connectivity, as described in "Viewing or Changing Wireless Settings".

4. Implement wireless security, as described in "Wireless Security".

For more information about wireless technology, see the link to the online document in "Wireless Communications" in Appendix C.

Wireless Placement and Range Guidelines

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

For best results, place your modem router according to the following guidelines:

- Near the center of the area in which your PCs will operate.

- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).

- Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.

- Away from large metal surfaces.

- Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.

- If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

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

Viewing or Changing Wireless Settings

You can view or change the wireless settings for the modem router. If you want to make changes, make sure to note the current settings first.

> **Note:** If you use a wireless computer to change the wireless settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the modem router from a wired computer to make further changes.

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

2. Select Wireless Settings from the main menu to display the Wireless Settings screen:

Figure 2-1

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

3. Select the region in which the modem router will operate.

4. For initial configuration and test, leave the other settings unchanged.

5. To save your changes, click **Apply**.

6. Configure and test your computers for wireless connectivity.

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

Table 2-1. Wireless Settings

Settings		Description
Wireless Network	Name (SSID)	The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a wireless network must use the SSID.
	Region	The location where the modem router is used.
	Channel	The wireless channel used by the gateway. The default is Channel 6. Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to experiment with different channels to see which is the best.
	Mode	The default is g & b, which allows both 802.11g and 802.11b wireless stations access. Note that in b only mode, 802.11g wireless stations can connect if they can operate in 802.11b mode.
Wireless Access Point	Enable Wireless Access Point	Selected by default, this setting enables the wireless radio, which allows the modem router to work as a wireless access point. Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting.
	Allow Broadcast Name (SSID)	Selected by default, the modem router broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the correct SSID. If you disable broadcast of the SSID, only devices with the correct SSID can connect. This nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. For this reason NETGEAR recommends that you also enable wireless security.
	Wireless Isolation	This feature is disabled by default. If it is enabled, wireless stations cannot communicate with each other or with stations on the wired network.

Table 2-1.   Wireless Settings (continued)

Settings		Description
Wireless Station Access List	Turn Access Control On	Access control is disabled by default so that any computer configured with the correct SSID can connect. See "Restricting Access by MAC Address".
Security Options		• **Disabled**. You can use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security. • **WEP (Wired Equivalent Privacy)**. WEP security uses encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. See "Configuring WEP". • **WPA2-PSK (Wi-Fi Protected Access Pre-Shared Key)**. Allow only computers configured with WPA2-PSK security to connect to the modem router. See "Configuring WPA". • **WPA-PSK + WPA2-PSK**. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the modem router. See "Configuring WPA". • **WPA-802.1x** and **WPA2-802.1**. Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.1x and Radius servers. See "Configuring WPA".

Wireless Security

Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The ADSL2+ Modem Wireless Router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

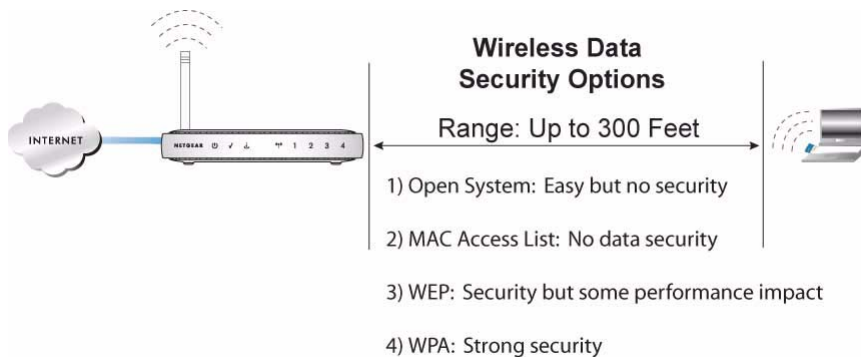There are several ways you can enhance the security of your wireless network:

Figure 2-2

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

- **Turn Off the Broadcast of the Wireless Network Name SSID**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network 'discovery' feature of some products, such as Windows XP, but the data is still exposed.

- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.

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

- **WPA-PSK (TKIP), WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise.

Wireless Station Access Control

By default, any wireless PC that is configured with the correct SSID and wireless security settings is allowed access to your wireless network. You can use Wireless Access Point settings in the Wireless Setting screen to further restrict wireless access to your network:

```
Wireless Access Point
☑ Enable Wireless Access Point
☐ Allow Broadcast of Name (SSID)
```

Figure 2-3

*   **Turning off wireless connectivity completely**.
    You can completely turn off the wireless portion of the modem router. For example, if you use your notebook computer to wirelessly connect to your router, and you take a business trip, you can turn off the wireless portion of the router while you are traveling. Other members of your household who use computers connected to the router via Ethernet cables can still use the router. To do this, clear the **Enable Wireless Access Point** check box on the Wireless Settings screen, and then click **Apply**.

*   **Hiding your wireless network name (SSID)**.
    By default, the modem router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To do this, clear the **Allow Broadcast of Name (SSID)** check box on the Wireless Settings screen, and then click **Apply**. Wireless devices will not "see" your modem router. You must configure your wireless devices to match the wireless network name (SSID) of the modem router.

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

*   **Restricting access by MAC address**.
    See "Restricting Access by MAC Address".

Restricting Access by MAC Address

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the ADSL2+ Modem Wireless Router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

To restrict access based on MAC addresses:

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

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

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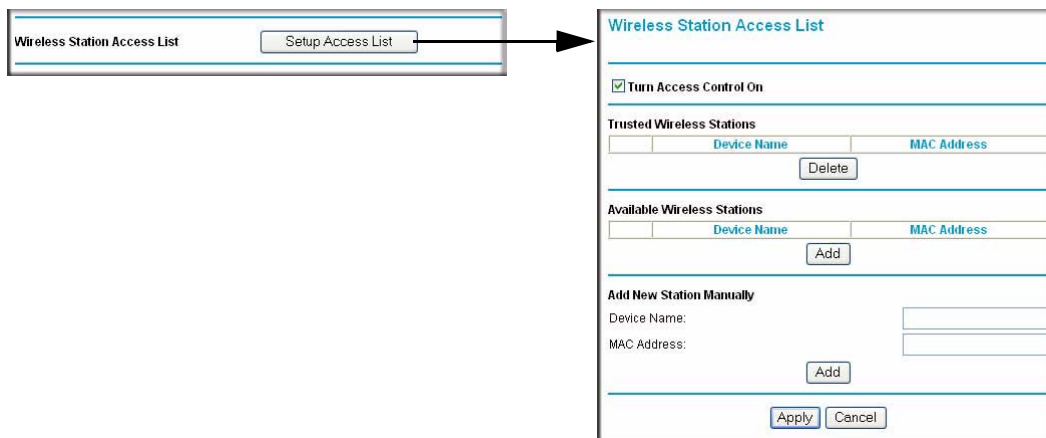

Figure 2-4

The trusted wireless stations listed on this screen are the wireless clients that will have access to the wireless network when the list is enabled.

3. Adjust the list as needed for your network. You can add devices to the Trusted Wireless Stations list using either of the following methods:

- If the computer is in the Available Wireless Stations table, select the radio button of that computer to capture its MAC address.

- Use the Add New Station Manually fields to enter the MAC address of the device to be added. The MAC address can usually be found on the bottom of the wireless device.

> **Note:** If no device name appears when you enter the MAC address, you can type a descriptive name for the computer that you are adding.

4. Click **Add**, and then click **Apply** to save these settings. Now, only devices on this list will be allowed to wirelessly connect to the modem router.

Configuring WEP

> **Note:** If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the modem router from a wired computer to make further changes.

To configure WEP data encryption:

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

2. From the main menu, select Wireless Settings to display the Wireless Settings screen.

3. In the Security Options section, select the **WEP (Wired Equivalent Privacy)** radio button:
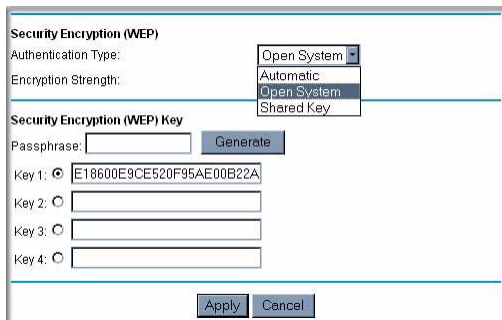

Figure 2-5

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

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

5. Select the **Encryption Strength** setting:
- **WEP (Wired Equivalent Privacy) 64-bit encryption**. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
- **WEP (Wired Equivalent Privacy) 128-bit encryption**. Enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).

6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network:
- **Passphrase**. To use a passphrase to generate the keys, enter a passphrase, and click **Generate**. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the modem router.

> **Note:** Not all wireless adapters support passphrase key generation.

- **Key 1-Key4**. These values are *not* case-sensitive. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).

7. Select which of the four keys will be the default.

   Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected.

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

Configuring WPA

WPA-PSK data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA makes it virtually impossible to compromise.

Not all wireless adapters support Wi-Fi Protected Access (WPA). Consult the product documentation for your wireless adapter for instructions for configuring WPA settings.

> **Note:** If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the modem router from a wired computer to make further changes.

To configure WPA in the modem router:

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

2. Select Wireless Settings from the main menu.

3. On the Wireless Setting screen, select the radio button for the WPA or WPA2 option of your choice.

4. The settings displayed on the screen depend on which security option you select.

5. For WPA-PSK or WPA2-PSK, enter the passphrase.

6. If prompted, enter the settings for the Radius server. These settings are required for communication with the primary Radius server. You can configure a secondary Radius server, which is used if the primary Radius server fails.

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

- **Radius Port**. Port number of the Radius server. The default is 1812.

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

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

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

Protecting Access to Your ADSL2+ Modem Wireless Router

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

> **Note:** The user name and password are not the same as a user name or password you might use to log in to your Internet connection.

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

Changing the Built-In Password

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

Figure 3-1

2. From the main menu, under the Maintenance heading, select Set Password to display the Set Password screen:
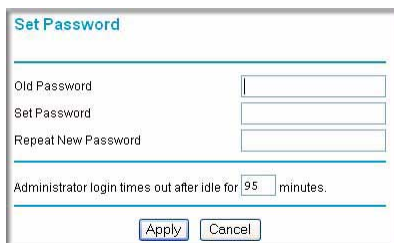
Set Password

Old Password

Set Password

Repeat New Password

Administrator login times out after idle for 95 minutes.

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

Changing the Administrator Login Time-out

For security, the administrator login to the modem router configuration times out after a period of inactivity. To change the login time-out period:

1. In the Set Password screen, type a number in the **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 in the following sections.

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 modem router prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for keywords within Web addresses. 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. 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 following section explains how to configure your modem router to perform these functions.

Blocking Keywords and Sites

The modem router allows you to restrict access to Internet content based on 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**, and default password of **password**, or using whatever password and LAN address you have chosen for the modem router.

2. On the main menu, select Block Sites to display the Block Sites screen:

Figure 3-3

3. To enable keyword blocking, select one of the following:

   • **Per Schedule**. Turn on keyword blocking according to the settings on the Schedule screen.

   • **Always**. Turn on keyword blocking all the time, independent of the setting in the Schedule screen.

4. Enter a keyword or domain in the **Keyword** field, click **Add Keyword**, and then click **Apply**.

   Some examples of keyword applications are shown in the following chart.

Keyword	Result
XXX	Block the URL http://www.badstuf.com/xxx.html.
.com	Only websites with other domain suffixes (such as .edu or .gov) can be viewed.
. (a period)	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**, and then click **Apply**.

6. To specify a trusted user, enter that computer's IP address in the **Trusted IP Address** field, and then click **Apply**.

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

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

Firewall Rules

Firewall rules 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.

The default inbound and outbound rules of the modem router 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" for more details.

To view or change firewall rules, select Firewall Rules on the main menu.

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 a rule to a different position in the table, select its button, and then click **Move**. At the prompt, enter the number of the desired new position, and then click **OK**.

Instant Messaging (IM) Ports

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

Inbound Rules (Port Forwarding)

Because the modem router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly access 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 broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP might periodically check for servers and might suspend your account if it discovers any active services at your location. If you are unsure, see the acceptable use policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Enable only 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 outside IP addresses to the IP address of your Web server at any time of day. This rule is shown in the following figure:

Figure 3-5

The settings 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 screen to add any additional services or applications that do not already appear.

v2.0, September 2007

- **Action**. Select when 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 screen.

- **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 option that you want:

  – **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 rule will be logged.

  – **Not match**. Traffic of this type that does not match the rule will be logged.

Inbound Rule Example: Allowing Videoconferencing

You can create an inbound rule to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office. In this example, CU-SeeMe connections are allowed only from a specified range of external IP addresses. This example also specifies logging of any incoming CU-SeeMe requests that do not match the allowed parameters.

Figure 3-6

Considerations for Inbound Rules

If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature so that external users can always find your network.

If the IP address of the local server computer is assigned by DHCP, it might 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 previous example). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

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

- 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)

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 screen. You can also have the modem router log any attempt to use Instant Messenger during that blocked period.

The following screen shows AIM selected in the **Service** list:

Figure 3-7

The Outbound Services screen includes the following fields:

- **Service**. Select the application or service from the drop-down list to be allowed or blocked. You can use the Add Custom Service feature to add any additional services or applications that are not in the list; see "Defining Services" for details.

- **Action**. Choose when you want this type of traffic to be handled. You can block or allow always, or you can block or allow according to the schedule defined in the Schedule screen.

- **LAN users**. This setting 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 fill in the **Start** and **Finish** fields.
  - **Single address**. Enter the required address in the Start field.

- **WAN users**. This setting determines which packets are covered by the rule, based on their destination WAN IP address. Select the option that you want:

  - **Any**. All IP addresses are covered by this rule.
  - **Address range**. If this option is selected, you must fill in the **Start** and **Finish** fields.
  - **Single address**. Enter the required address in the **Start** field.

- **Log**. 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 rule will be logged.
  - **Not match**. Traffic of this type that does not match the rule will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Firewall Rules screen, as shown:

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 might 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 RFC 1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the modem router already holds a list of many service port numbers, you are not limited to these choices. Use the following procedure to define your own services.
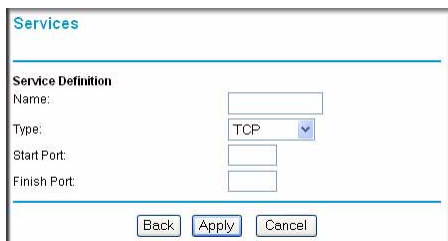
Defining Services

To define a service:

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. Under the Security heading, select Services to display the Services screen:

Figure 3-9

- To create a new service, click **Add Custom Service**.

- To edit an existing service, select its button on the left side of the table, and then click **Edit Service**.

- To delete an existing service, select its button on the left side of the table, and then click **Delete Service**.

3. Use the screen shown in the following figure to define or edit a service.

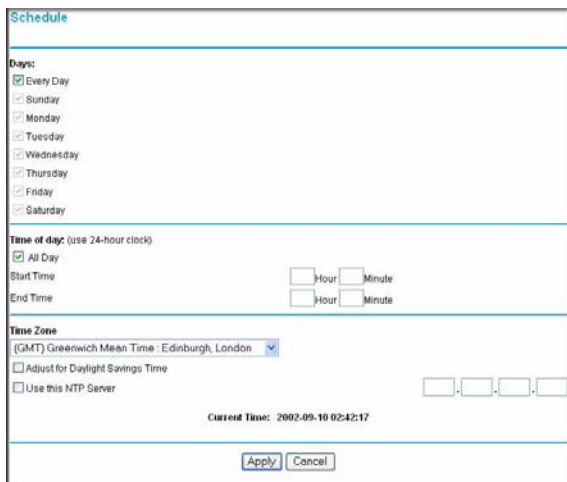**Figure 3-10**

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

Setting Times and Scheduling Firewall Services

The modem router uses network time protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

Setting Your Time Zone

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. On the main menu, select Schedule to display the Schedule screen:

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.

If your time zone is currently in daylight savings time, select the **Adjust for daylight savings time** check box.

> → **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 causes 1 hour to be added to the standard time.

4. The modem router has a list of NETGEAR NTP servers. If you prefer to use a particular NTP server as the primary server, enter its IP address in the **Use this NTP Server** field.

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

Scheduling Firewall Services

If you enabled services blocking in the Block Services screen or port forwarding in the Ports screen, 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. On the main menu, select the Schedule. The Schedule screen appears.

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, fill in the **Start Blocking** and **End Blocking** fields.

4. Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. 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.
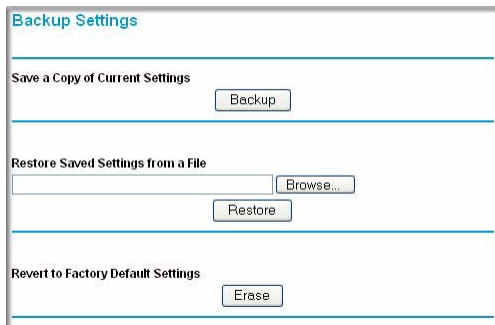
This chapter describes how to perform network management tasks with your ADSL2+ Modem Wireless Router.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the 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.

Backing 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. Under the Maintenance heading on the main menu, select Backup Settings to display the Backup Settings screen:

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.

Restoring the Configuration from a File

To restore the configuration:

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. Under the Maintenance heading on the main menu, select Backup Settings.

3. Enter the full path to the file on your network, or click **Browse** to locate the file.

4. When you have located the .cfg file, click **Restore** to upload the file to the modem router.

5. The modem router reboots.

Erasing the Configuration

You can use the Erase feature to erase its configuration settings and restore the modem router to the factory default settings.

To erase the configuration:

1. Under the Maintenance heading on the main menu select, Backup Settings.

2. Click **Erase**.

3. The modem router reboots.

   After an erase, the modem router password is **password**, the LAN IP address is **192.168.0.1**, and the modem router DHCP client is enabled.

> **Note:** To restore the factory default configuration settings when you do not know the login password or IP address, use the reset button on the rear panel of the modem router.

Upgrading the Modem Router Firmware

The software of the modem router is stored in flash memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR website. If the upgrade file is compressed (a .zip file), you must first extract the binary (.bin or .img) file before uploading it to the modem router.

Upgrading the Modem Router Firmware

NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you might 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 later, or Netscape Navigator 4.7 or later.

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, under the Maintenance heading, select Router Upgrade to display the Firmware Upgrade screen:
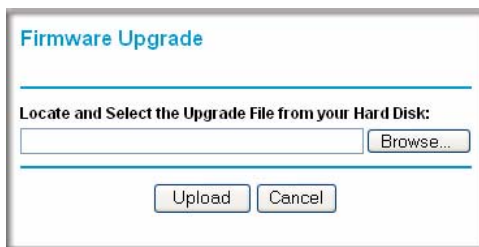
Figure 4-2

4. Click **Browse** to locate the binary (.bin or .img) upgrade file.

5. Click **Upload**.

> ⚠ **Warning:** When uploading software to the modem router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it might corrupt the software. When the upload is complete, your modem router will automatically restart. The upgrade process typically takes about 1 minute. In some cases, you might need to clear the configuration and reconfigure the modem router after upgrading.

Network Management Information

The modem router provides a variety of status and usage information which is discussed below.

Viewing Modem Router Status and Usage Statistics

From the main menu, below the Maintenance heading, select Router Status to view this screen.

Figure 4-3

The Router Status screen provides status and usage information. This screen shows the following parameters:

Table 4-1.   Modem Router Status Fields

Field	Description
Account Name	The host name assigned to the modem router in the Basic Settings screen.
Firmware Version	This field displays the modem router firmware version.

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

Field		Description
ADSL Port	MAC Address	The Ethernet MAC address used by the ADSL port of the modem router.
	IP Address	The IP address used by the ADSL port. If no address is shown, the modem router cannot connect to the Internet.
	Network Type	The network type is determined by your ISP. Common network types are PPPoE and PPPoA.
	IP Subnet Mask	The IP subnet mask used by the ADSL port.
	Domain Name Server (DNS)	The DNS server IP addresses used by the modem router. These addresses are usually obtained dynamically from the ISP.
LAN Port	MAC Address	The Ethernet MAC address used by the local (LAN) port of the modem router.
	IP Address	The IP address used by the local (LAN) port. The default is 192.168.0.1.
	DHCP	• **Off:** The modem router will not assign IP addresses to PCs on the LAN. • **On:** The modem router assigns IP addresses to PCs on the LAN.
	IP Subnet Mask	The IP subnet mask used by the local (LAN) port. The default is 255.255.255.0.
Modem	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.

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

Field		Description
Wireless Port These are set in the Wireless Settings page; see "Viewing or Changing Wireless Settings" in Chapter 2.	Name (SSID)	The service set ID, also known as the wireless network name.
	Region	The country where the unit is set up for use.
	Channel	The current channel, which determines the operating frequency.
	Wireless AP	Indicates if the access point feature is disabled or not. If not enabled, the Wireless LED on the front panel will be off.
	Broadcast Name	Indicates if the DG834G v4 is configured to broadcast its SSID.

Viewing Statistics

Click the **Show Statistics** button on the Router Status screen to display modem router usage statistics:

Figure 4-4

This following table explains the statistic fields.

Table 4-2.   Router Statistics Fields

Field		Description
WAN or LAN Port The statistics for the WAN (Internet) and LAN ports.	Status	The link status of the port.
	TxPkts	The number of packets transmitted on this port since reset or manual clear.
	RxPkts	The number of packets received on this port since reset or manual clear.
	Collisions	The number of collisions on this port since reset or manual clear.
	Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
	Rx B/s	The average line utilization for this port.
	Up Time	The time elapsed since the last power cycle or reset.
ADSL Link Downstream or Upstream These statistics might help your technical support representative if there is a connection problem.	Connection Speed	Typically, the downstream speed is faster than the upstream speed.
	Line Attenuation	The line attenuation increases 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.

Connection Status

Click the **Connection Status** button on the Router Status screen to view the connection status:

Figure 4-5
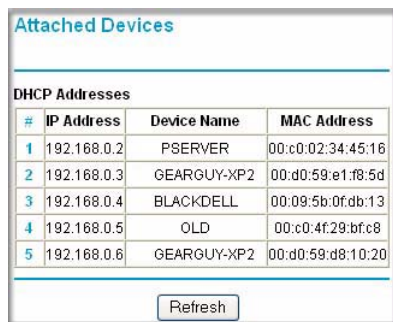
This screen shows the following statistics:

Table 4-3.   Connection Status Fields for PPPoA

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

Viewing Attached Devices

The Attached Devices screen contains a table of all IP devices that the modem router has discovered on the local network. From the main menu, under the Maintenance heading, select Attached Devices. The Attached Devices screen displays:

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 logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites screen, the Logs screen can show you when someone on your network tries to access a blocked site. If you enabled e-mail notification, you 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 in the following figure:

Figure 4-7

Log entries are described in the following table.

Table 4-4. Security Log Entry Descriptions

Field	Description
Current time	The date and time the log entry was recorded.
Description or action	The type of event and what action was taken if any.

Table 4-4. Security Log Entry Descriptions

Field	Description
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 website.
Destination port and interface	The service port number of the destination device, and whether it is on the LAN or WAN.

Log action buttons are described in the following table.

Table 4-5. 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 Which Information to Log

Besides the standard information listed previously, 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 the **Broadcast on LAN** radio button 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 e-mailed.]

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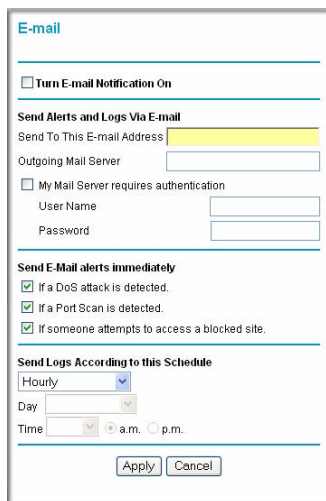
[These entries show an inbound FTP (port 21) packet, User Datagram Protocol (UDP) packet (port 6970), and Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

Enabling Security Event E-mail Notification

To receive logs and alerts by e-mail, you must provide your e-mail information in the E-mail screen:

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).

  – **My Mail Server requires authentication**. Select this check box if you need to log in to your SMTP server to send E-mail. If you select this feature, you must enter the user name and password for the mail server.

  > **Tip:** If you cannot remember this information, 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.

    – **Time for sending log**. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.
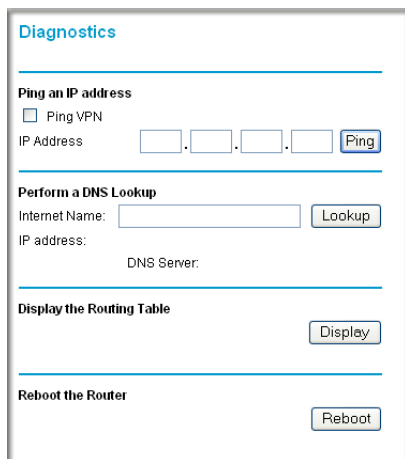
    If the **Weekly**, **Daily**, or **Hourly** option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot e-mail the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.

Running Diagnostic Utilities and Rebooting the Modem Router

The modem router has a diagnostics feature. You can use the Diagnostics screen to perform the following functions from the modem router:

- Ping an IP address to test connectivity to see if you can reach a remote host. If Ping VPN is enabled, the ping packet always goes through the VPN if the VPN tunnel is enabled and working.

- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.

- Display the routing table to identify what other modem routers the modem router is communicating with.

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

From the main menu, under the Maintenance heading, select Modem Router Diagnostics to display the Diagnostics screen:

Figure 4-9

Enabling Remote Management

Using the Remote Management screen, you can allow a user or users on the Internet to configure, upgrade, and check the status of your modem router.

> **Tip:** Be sure to change the modem router 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-case 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. Under the Advanced heading of the main menu, select Remote Management to display the Remote Management screen:
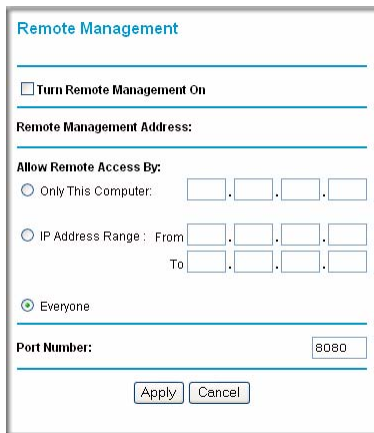
Figure 4-10

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

4. Specify which 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 field 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 WAN IP address in your Internet browser address or location field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter:

http://134.177.0.123:8080

Note: In this case, you must include http:// in the address.

Chapter 5
Advanced Configuration

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

Advanced Settings

The ADSL2+ Modem Wireless Router provides a variety of advanced features, such as the following:

- WAN Setup.
- LAN TCP/IP settings
- Using the Router as a DHCP Server
- Configuring Dynamic DNS
- Configuring Static Routes.
- Wireless Bridging and Repeating

These features are discussed in the following sections of this chapter.

WAN Setup

To view or change the WAN Setup:

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

2. From the main menu, select WAN Setup to display the WAN Setup screen:

Figure 5-1

3. Make the changes that you want, and then click **Apply** to save the settings.

The WAN Setup fields are described in the following table:

Table 5-1.   WAN Setup Settings

Setting	Description
Connect Automatically, as Required	Usually, this check box is selected, so that an Internet connection is made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting. • If disabled, you must connect manually, using the screen accessed from the **Connection Status** button on the Router Status screen. • If you have an "Always on" connection, this setting has no effect.
Enable PPPOE-RELAY	If this check box is selected, this feature allows a PPPoE client on a local PC to a remote PPPoE server with the gateway acting as a relay agent.
Disable Port Scan and DOS Protection	This check box is usually clear so that the firewall protects your LAN against port scans and denial of service (DOS) attacks. This check box should be selected only in special circumstances.
Default DMZ Server	This feature is sometimes helpful when you are using some online games and videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See "Setting Up a Default DMZ Server" on page 5-3.

Table 5-1.   WAN Setup Settings

Setting	Description
Respond to Pin on Internet WAN Port	If you want the modem router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, since it allows your modem router to be discovered. Do not select this check box unless you have a specific reason to do so.
MTU Size (in bytes)	The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 Bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Setting Up a Default DMZ Server

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

The default DMZ server feature is helpful when you are 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.

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 screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

To assign a computer or server to be a default DMZ server:

1. Go to the WAN Setup screen as described in the previous section.

2. Select the **Default DMZ Server** check box.

3. Type the IP address for that server.

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

LAN IP Settings

The LAN IP Setup screen allows configuration of LAN IP services such as DHCP and RIP. These features can be found under the Advanced heading in the modem router main menu.

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 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 screen.

To view or change the LAN IP Setup:.

⚠	**Warning:** If you change the LAN IP address of the modem router while connected through the browser, you will be disconnected and so will others connected to the router. To connect to the router, you must open a new connection to the new IP address and log in again. Others using the router must restart their computers to connect to the router again.

1. Select LAN IP to display the LAN IP Setup screen:

Figure 5-2

2. Change the settings. For more information, see Table 5-2, "DHCP Settings" on page 5-6 or "Reserved IP Addresses" on page 5-7.

3. Click **Apply** to save the changes.

The LAN TCP/IP Setup parameters are explained in the following table.

Table 5-2.   LAN IP Setup

Settings		Description
LAN TCP/IP Setup	IP Address	The LAN IP address of the modem router.
	IP Subnet Mask	The LAN subnet mask of the modem router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router.
	RIP Direction	RIP (Router Information Protocol) allows a modem router to exchange routing information with other routers. This setting controls how the modem router sends and receives RIP packets. **Both** is the default. • **Both** or **Out Only**. The modem router broadcasts its routing table periodically. • **Both** or **In Only**. The modem router incorporates the RIP information that it receives. • **None**. The modem router will not send any RIP packets and will ignore any RIP packets received.
	RIP Version	This controls the format and the broadcasting method of the RIP packets that the modem router sends. It recognizes both formats when receiving. By default, this is **RIP-1**. • RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup. • RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.
DHCP Server For more information, see "DHCP Settings" on page 5-6.	Use Router as a DHCP Server	This check box is usually selected so that the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server. See "DHCP Settings" on page 5-6.
	Starting IP Address	Specify the start of the range for the pool of IP addresses in the same subnet as the modem router.
	Ending IP Address	Specify the end of the range for the pool of IP addresses in the same subnet as the modem router.
Address Reservation For more information, see "DHCP Settings" on page 5-6.		When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it access the router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

DHCP Settings

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

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See the online document listed in "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 on the LAN IP Setup screen. Otherwise, leave it selected.

Specify the pool of IP addresses to be assigned by filling in the **Starting IP Address** and **Ending IP Address** fields. 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 might want to save part of the range for devices with fixed addresses.

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

- An IP address from the range you have defined.

- Subnet mask.

- Gateway IP Address is the router's LAN IP address.

- Primary DNS server, if you entered a primary DNS address in the Basic Settings screen; otherwise, the router's LAN IP address.

- Secondary DNS server, if you entered a secondary DNS address in the Basic Settings screen.

- WINS Server (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 always receives 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** field, 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 screen 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**.

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 to register your domain to their IP address, and 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.

Configuring Dynamic DNS

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

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

2. From the main menu, select Dynamic DNS to display the Dynamic DNS screen:

Figure 5-3

3. Access the website of one of the Dynamic DNS service providers whose names appear in the **Service Provider** drop-down list, 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. Fill in the **Host Name**, **User Name**, and **Password** fields.

   The dynamic DNS service provider may call the host name a domain name. If your URL is myName.dyndns.org, then your host name is myName. The password can be a key for your dynamic DNS account.

7. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature.

   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.

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

Using Static Routes

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

Static Route Example

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

- Your primary Internet access is through a cable modem to an ISP.

- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.

- Your company's network is 134.177.0.0.

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

In this case you must define a static route, telling your 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 5-5.

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.

- In the **Metric** field, a 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.

Configuring 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** and 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 the Advanced heading, select Static Routes to view the Static Routes screen:

Figure 5-4

3. Click **Add** or **Edit** to display the following screen:

Figure 5-5

4. Fill in or change the fields:

   • **Route Name.** The route name is for identification purposes only.

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

   • **Active**. Select this check box to make this route effective.

   • **Destination IP Address**, and **IP Subnet Mask**. If the destination is a single host, type a
   subnet value of **255.255.255.255**.

   • **Gateway IP Address**. This must be a router on the same LAN segment as the modem
   router.

   • **Metric**. Type a number between 2 and 15. 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 2.

5. Click **Apply** to either save your changes. If you added a static route, it is added to the Static
   Routes screen.

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. Select UPnP on the main menu to display the UPnP screen:

Figure 5-6

2. Fill in the settings on 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 modem router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the modem router.

- **Advertisement Period**. The advertisement period is how often the modem router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.

- **Advertisement Time To Live**. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. 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 might 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 modem 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 your changes, or refresh the table:

- Click **Apply** to save the new settings to the modem router.
- Click **Cancel** to disregard any unsaved changes.
- Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Wireless Bridging and Repeating

You can build large bridged wireless networks by using the modem router to configure a wireless distribution system (WDS).

Here are some examples of wireless bridged configurations:

*   **Point-to-Point bridge**. The modem router communicates with another bridge-mode wireless station. See "Point-to-Point Bridge Configuration".

*   **Multi-Point bridge**. The modem router is the "master" for a group of bridge-mode wireless stations. Then all traffic is sent to this "master," rather than to other access points. See "Multi-Point Bridge Configuration".

*   **Repeater with wireless client association**. Sends all traffic to the remote access point. See "Repeater with Wireless Client Association".

> **Note:** The wireless bridging and repeating feature uses the default security profile to send and receive traffic.

To view or change these configurations, select Advanced Wireless Settings from the main menu:

Figure 5-7

Point-to-Point Bridge Configuration

In Point-to-Point Bridge mode, the DG834G v4 modem router communicates as an access point with another bridge-mode wireless station. As a bridge, wireless client associations are disabled— only wired clients can be connected. You must enter the MAC address of the other bridge-mode wireless station in the field provided. Use wireless security to protect this communication.

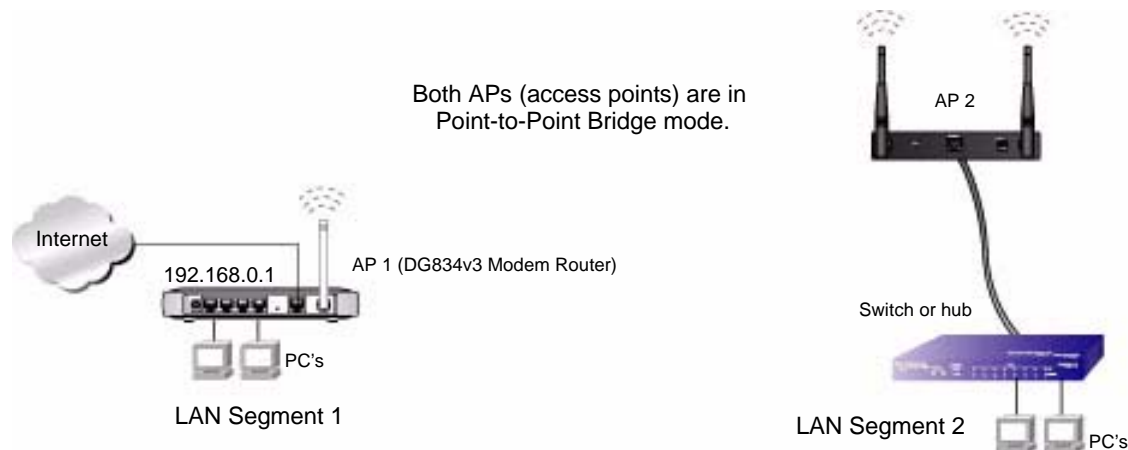The following figure shows an example of Point-to-Point Bridge mode.

Figure 5-8

To set up a point-to-point bridge configuration (shown in Figure 5-8):

1. Configure the DG834G v4 modem router (AP 1) on LAN Segment 1 in Point-to-Point Bridge mode.

2. Configure the other access point (AP 2) on LAN Segment 2 in Point-to-Point Bridge mode.

The DG834G v4 modem router must have AP 2's MAC address in its **Remote MAC Address** field, and AP 2 must have the DG834G v4's MAC address in its **Remote MAC Address** field.

3. Configure and verify the following for both access points:

   • Both APs must use the same SSID, channel, authentication mode, if any, and security settings if security is in use.

4. Disable the DHCP server on AP2. AP1 will then be the DHCP server.

5. Verify connectivity across LAN Segment 1 and LAN Segment 2.

A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

Multi-Point Bridge Configuration

Multi-Point Bridge mode allows a modem router to bridge to multiple peer access points simultaneously. As a bridge, wireless client associations are disabled—only wired clients can be connected. Multi-Point Bridge mode configuration includes the following steps:

• Entering the MAC addresses of the other access points in the fields provided.

• Setting the other bridge-mode access points to Point-to-Point Bridge mode, using the MAC address of this DG834G v4 as the Remote MAC Address.

• Using wireless security to protect this traffic.

The figure below shows an example of a Multi-Point Bridge mode configuration.

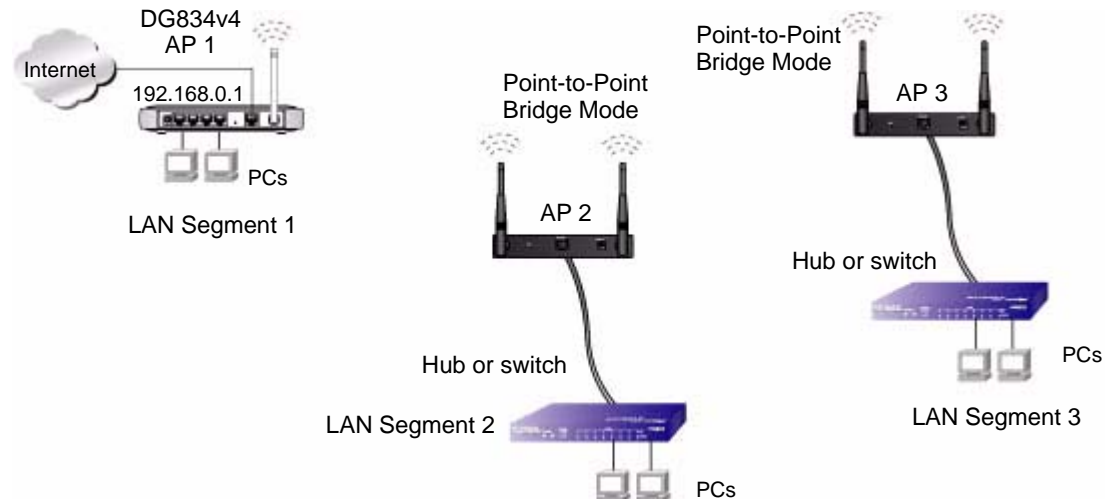**The DG834v4 is AP 1, which is the "Master AP" in Point-to-Multi-Point Bridge mode.**

Figure 5-9

To set up the multi-point bridge configuration shown in Figure 5-9:

1. Configure the operating mode of the modem routers.

• Because it is in a central location, configure the DG834G v4 modem router (AP 1) on LAN Segment 1 in Point-to-Multi-Point Bridge mode and enter the MAC addresses of AP 2 and AP 3 in the **Remote MAC Address 1** and **Remote MAC Address 2** fields.

• Configure the access point (AP2) on LAN Segment 2 in Point-to-Point Bridge mode with the remote MAC address of the DG834G v4 modem router.

- Configure the access point (AP3) on LAN Segment 3 in Point-to-Point Bridge mode with the remote MAC address of the DG834G v4 modem router.

2. Disable the DHCP server on AP2 and AP3. AP1 will then be the DHCP server.

3. Verify the following for all access points:

   - The LAN network configuration of the modem router and other access points are configured to operate in the same LAN network address range as the LAN devices.

   - Only one AP, the DG834G v4 modem router in Figure 5-9, is configured in Point-to-Multi-Point Bridge mode; all the others are in Point-to-Point Bridge mode.

   - All APs, including the DG834G v4 modem router, must be on the same LAN. That is, all the AP LAN IP addresses must be in the same network.

   - If using DHCP, all access points should be set to **Obtain an IP address automatically (DHCP Client)** in the IP Address Source section of the Basic IP Settings screen.

   - All APs, including the DG834G v4 modem router, must use the same SSID, channel, authentication mode, if any, and encryption in use.

   - All point-to-point APs must have the MAC address of AP 1 (the DG834G v4 modem router in the above diagram) in the **Remote AP MAC address** field.

4. Verify connectivity across the LANs.

   - A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.

> **Note:** Wireless stations configured as they are in Figure 5-9 will not be able to connect to the modem router or access points. If you require wireless stations to access any LAN segment, you can use additional access points configured in Wireless Access Point mode in any LAN segment.

Repeater with Wireless Client Association

In this mode, the ADSL2+ Modem Wireless Router sends all traffic to a remote AP. For Repeater mode, you must enter the MAC address of the remote "parent" access point. Alternatively, you can configure the ADSL2+ Modem Wireless Router as the parent by entering the address of a "child" access point. Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this ADSL2+ Modem Wireless Router.

• You cannot configure a sequence of parent/child APs. You are limited to only one parent AP, although if the DG834G v4 is the parent AP it can connect with up to four child APs.

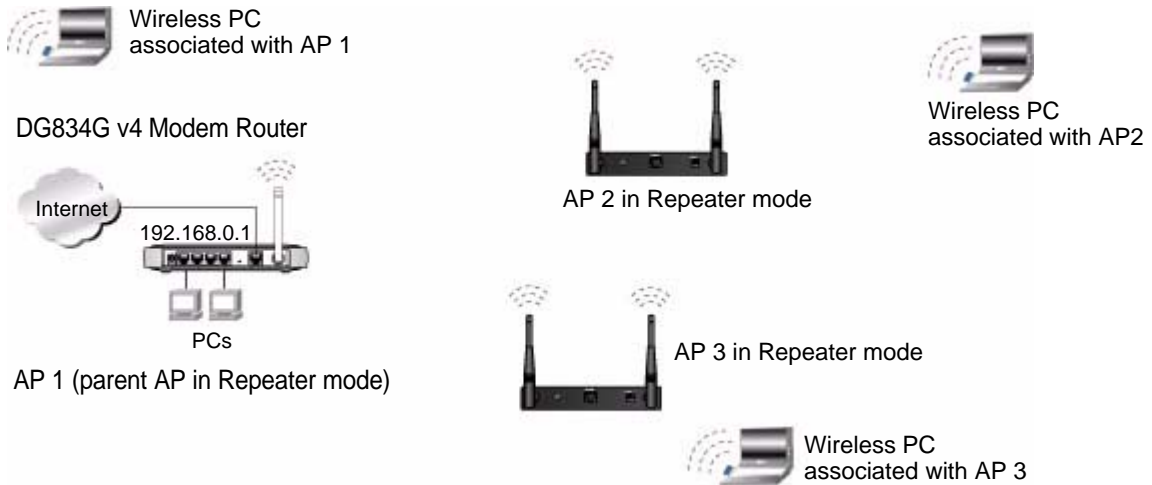The following figure shows an example of a Repeater Mode configuration.

Figure 5-10

To set up a repeater with wireless client association:

1. Configure the operating mode of the devices.

   • Configure AP 1 the DG834G v4 modem router in the previous figure) on LAN Segment 1 with the MAC address of AP 2 and AP 3 in the first two **Remote MAC Address** fields.

   • Configure AP 2 with the MAC address of AP 1 in the **Remote MAC Address** field.

   • Configure AP 3 with the MAC address of AP 1 in the **Remote MAC Address** field.

2. Verify the following for both access points:

   • The LAN network configuration of each AP is configured to operate in the same LAN network address range as the LAN devices.

   • The APs must be on the same LAN. That is, the LAN IP addresses for the APs must be in the same network.

   • If you are using DHCP, AP devices should be set to **Obtain an IP address automatically (DHCP Client)** in the IP Address Source section of the Basic IP Settings screen.

   • AP devices must use the same SSID, channel, authentication mode, and encryption.

3. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

This chapter describes how to use the virtual private networking (VPN) features of the ADSL2+ Modem Wireless Router. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer. See "Virtual Private Networking (VPN)" in Appendix C to learn more about VPN.

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.

- "Setting Up a Client-to-Gateway VPN Configuration" on page 6-5 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.

- "Setting Up a Gateway-to-Gateway VPN Configuration" on page 6-18 provides the steps needed to configure a VPN tunnel between two network gateways using the VPN Wizard.

- "VPN Tunnel Control" on page 6-25 provides the step-by-step procedures for activating, verifying, deactivating, and deleting a VPN tunnel once the VPN tunnel has been configured.

- "Setting Up VPN Tunnels in Special Circumstances" on page 6-32 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 PC and a network gateway; and between two or more network gateways. The DG834G v4 supports both of these types of VPN configurations. The DG834G v4 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.
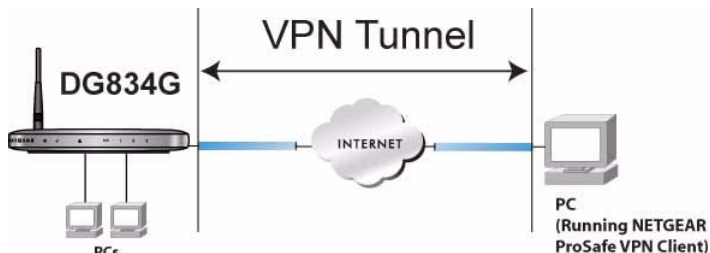

Figure 6-1

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 modem router on your network is the other tunnel endpoint. See "Setting Up a Client-to-Gateway VPN Configuration" on page 6-5 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.
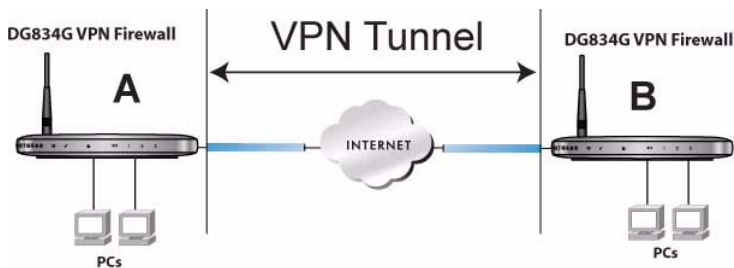

Figure 6-2

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 DG834G v4s on each end of the tunnel to form the VPN tunnel end points. See "Setting Up a Gateway-to-Gateway VPN Configuration" on page 6-18 for information about how 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 "Using a Fully Qualified Domain Name (FQDN)" on page B-7) 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.

- Which 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 6-32)

  – A manual keying setup in which you must specify each phase of the connection (see "Using Manual Policy to Configure VPN Tunnels" on page 6-41)?

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.

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 "Setting Up a Client-to-Gateway VPN Configuration" on page 6-5.

    – See "Setting Up a Gateway-to-Gateway VPN Configuration" on page 6-18.

- See "Using Auto Policy to Configure VPN Tunnels" on page 6-32 when the VPN Wizard and its VPNC defaults (see Table 6-2) 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 6-41 when the VPN Wizard and its VPNC defaults (see Table 6-2) 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 DG834G v4 and the corresponding VPN endpoint gateway or client workstation.

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

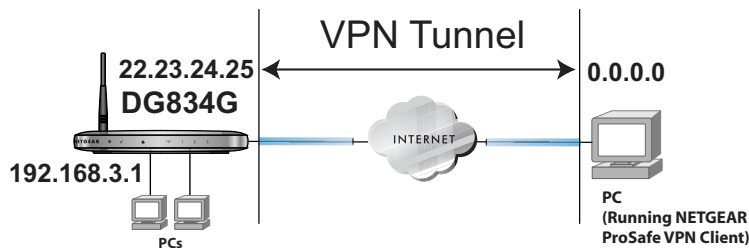# Setting Up a Client-to-Gateway VPN Configuration

Figure 6-3

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

- "Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834G v4" on page 6-6 describes how to use 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 6-9 shows how to configure the NETGEAR ProSafe VPN Client endpoint.

Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834G v4

→ **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 "Setting Up VPN Tunnels in Special Circumstances" on page 6-32 to set up the VPN tunnel.

The worksheet in Table 6-3 identifies the parameters used in the following procedure. A blank worksheet is at "Planning a VPN".

Table 6-3.   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**
DG834G v4	**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 modem router at its LAN address of **http://192.168.0.1** with its default user name of **admin** and password of **password**. On the main menu, select VPN Wizard. The VPN Wizard screen displays:
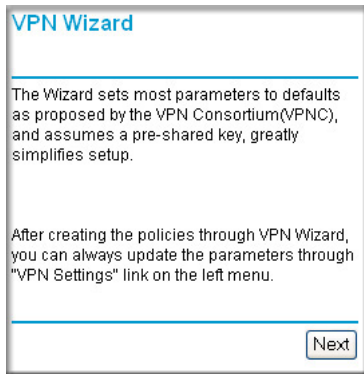

Figure 6-4

2. Click **Next** to proceed. Fill in the **Connection Name** and the **pre-shared key** fields. Select the radio button for the type of target end point, and then click **Next** to proceed.
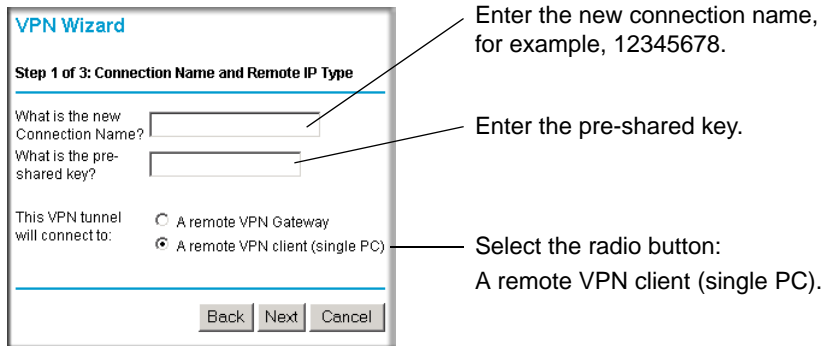

Enter the new connection name, for example, 12345678.

Enter the pre-shared key.

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

Figure 6-5

> **Tip:** The connection name is arbitrary and not relevant to how the configuration functions.

The Summary screen displays:

Figure 6-6

To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the **here** link. You can click **Back** to return to the Summary screen.

Figure 6-7

3. Click **Done** on the Summary screen to complete the configuration procedure. The VPN Policies screen 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:** See "Using Auto Policy to Configure VPN Tunnels" on page 6-32 to enable the IKE keepalive 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. These instructions assume that 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*) for information about 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 might be running on your PC. You might need to insert your Windows CD to complete the installation.

1. Install the NETGEAR ProSafe VPN Client on the remote PC, and then reboot.

    a. Install the IPSec component. You might have the option to install either the VPN adapter or the IPSec component or both. The VPN adapter is not necessary.

v2.0, September 2007

If you do not have a modem or dial-up adapter installed in your PC, you might see the warning message stating "The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed." You can disregard this message.

b. Reboot the remote PC.

The ProSafe icon (⬛) is in the system tray.

c. Double-click the ProSafe icon to open the Security Policy Editor.

2. Add a new connection.

a. Run the NETGEAR ProSafe Security Policy Editor program, and, using the "VPN Tunnel Configuration Worksheet" on page 6-6, create a VPN connection.

b. From the Edit menu of the Security Policy Editor, click **Add**, and then click **Connection**.
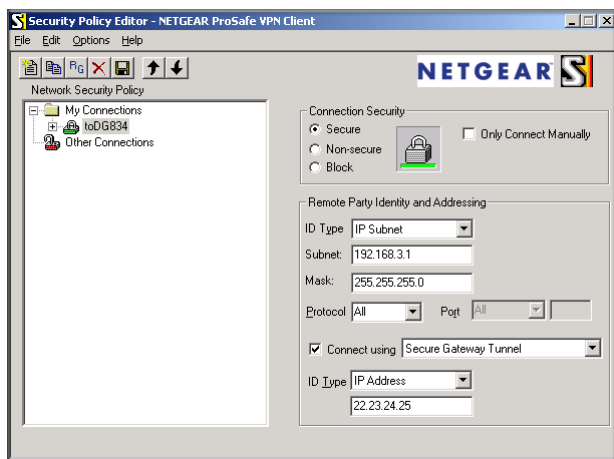

Figure 6-9

A New Connection listing appears in the list of policies. Rename the New Connection so that it matches the **Connection Name** field in the VPN Settings screen of the DG834G v4 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 because connection names are irrelevant to how the VPN tunnel functions.
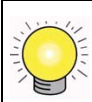
> **Tip:** Choose connection names that make sense to the people using and administering the VPN.

c. Enter the following settings:

- Connection Security: **Secure**.
- **ID Type**: **IP Subnet**.
- **Subnet**: In this example, type **192.168.3.1** as the network address of the DG834G v4.
- **Mask**: Enter **255.255.255.0** as the LAN Subnet Mask of the DG834G v4.
- **Protocol**: Select **All** to allow all traffic through the VPN tunnel.

d. Select the **Connect using Secure Gateway Tunnel** check box.

e. Select **IP Address** in the **ID Type** drop-down list.

f. Enter the public WAN IP Address of the DG834G v4 in the field directly below the **ID Type** drop-down list. In this example, **22.23.24.25** is used.

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 the + symbol. My Identity and Security Policy subheadings appear below the connection name.

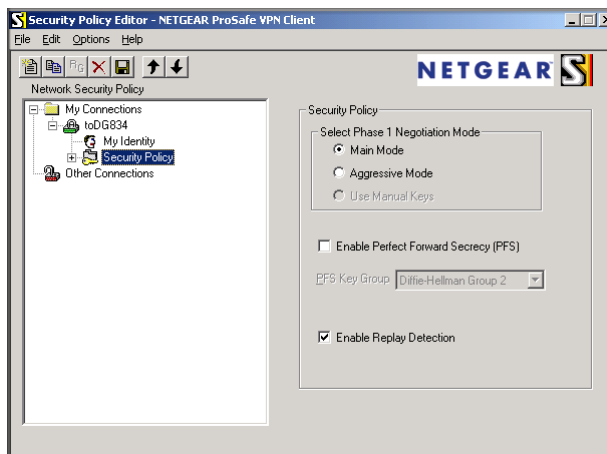**b.** Click the **Security Policy** subheading to view the Security Policy settings.

Figure 6-10

    c. In the Select Phase 1 Negotiation Mode section of the screen, select the **Main Mode** radio button.

4. Configure the VPN client identity.

In this step, you provide information about the remote VPN client PC. You must provide the pre-shared key that you configured in the DG834G v4 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**.
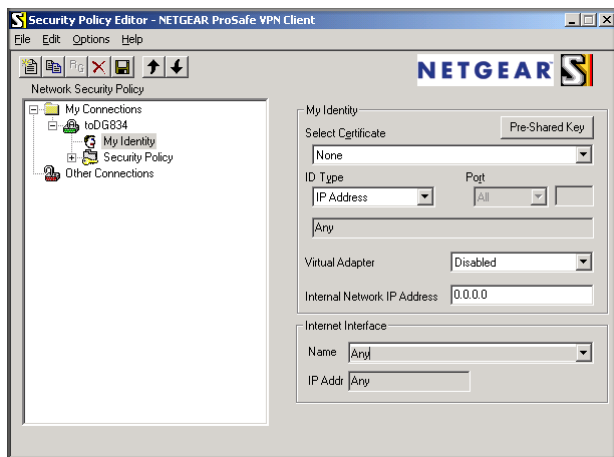

Figure 6-11

    b. In the **Select Certificate** drop-down list, select **None**.

    c. Select **IP Address** in the **ID Type** drop-down list. If you are using a virtual fixed IP address, enter this address in the **Internal Network IP Address** field. Otherwise, leave this field empty.

    d. In the Internet Interface section of the screen, select the adapter that you use to access the Internet. If you have a dial-up Internet account, select **PPP Adapter** in the **Name** field. If you have a dedicated cable or DSL line, select your Ethernet adapter. If you will be switching between adapters or if you have only one adapter, select **Any**.

e. In the My Identity section of the screen, click the **Pre-Shared Key** button. The Pre-Shared Key screen displays:
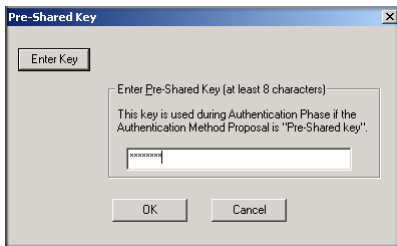

Figure 6-12

f. Click **Enter Key**. Enter the DG834G v4 pre-shared key, and then click **OK**. In this example, **12345678** is entered. This field is case-sensitive.

5. Configure the VPN Client Authentication Proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the DG834G v4 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 the + symbol.

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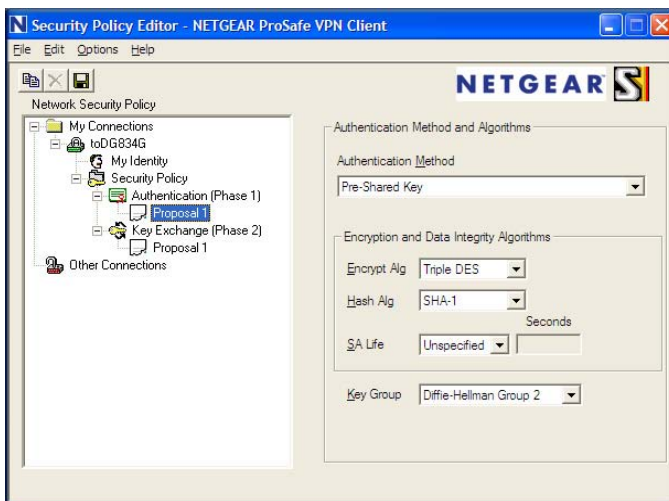

Figure 6-13

   c. In the Authentication Method drop-down list, select **Pre-Shared key**.

   d. In the **Encrypt Alg** drop-down list, select the type of encryption that is configured for the Encryption Protocol in the DG834G v4 in Table 6-3 on page 6-6. In this example, use Triple DES.

   e. In the **Hash Alg** drop-down list, select **SHA-1**.

   f. In the **SA Life** drop-down list, select **Unspecified**.

   g. In the **Key Group** drop-down list, select **Diffie-Hellman Group 2**.

6. Configure the VPN client key exchange proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the DG834G v4 configuration.

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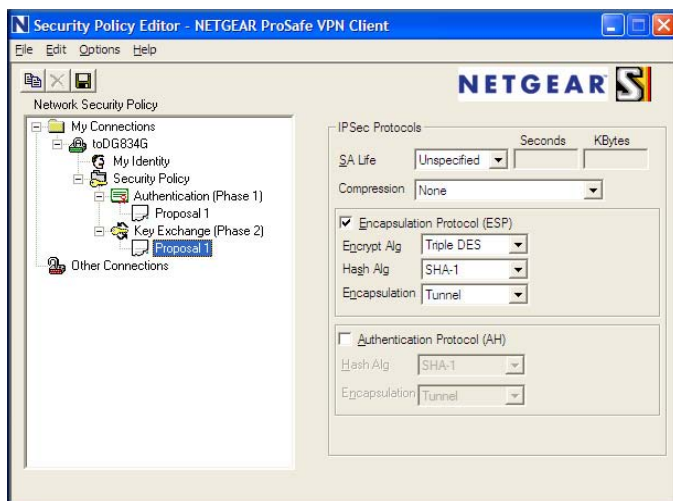

Figure 6-14

   b. In the **SA Life** drop-down list, select **Unspecified**.

   c. In the **Compression** drop-down list, select **None**.

   d. Select the **Encapsulation Protocol (ESP)** check box.

   e. In the **Encrypt Alg** drop-down list, select the type of encryption that is configured for the Encryption Protocol in the DG834G v4 in Table 6-3 on page 6-6. In this example, use Triple DES.

f. In the **Hash Alg** drop-down list, select **SHA-1**.

g. In the **Encapsulation** drop-down list, select **Tunnel**.

h. Leave the **Authentication Protocol (AH)** check box cleared.

7. Save the VPN Client Settings.

In the Security Policy Editor window, select File > Save.

After you have configured and saved the VPN client information, your PC automatically opens 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 DG834G v4 modem router's network by using the Connect option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client reports 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**.

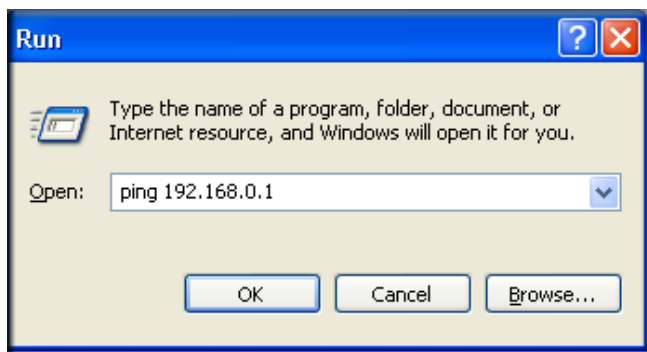**c.** Type **ping -t 192.168.3.1**, and then click **OK**.

Figure 6-15

This causes a continuous ping to be sent to the first DG834G v4. After between several seconds and two minutes, the ping response should change from `timed out` to `reply`.

Figure 6-16

Once the connection is established, you can open a browser on the PC and enter the LAN IP address of the remote DG834G v4. After a short wait, you should see the login screen of the modem router (unless another PC already has the DG834G v4 management interface open).

You can view information about the progress and status of the VPN client connection by opening the NETGEAR ProSafe Log Viewer.

To launch this function, click the Windows **Start** button, then select Programs > NETGEAR ProSafe VPN Client > Log Viewer. The Log Viewer screen for a successful connection is shown in the following figure:
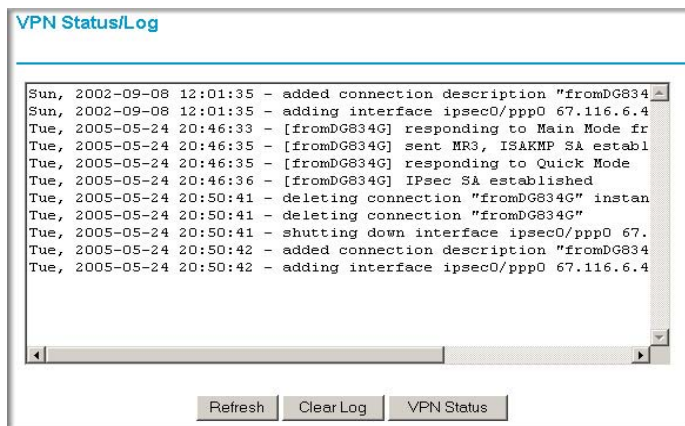

Figure 6-17

> **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.

9. The Connection Monitor screen for this connection is shown in the following figure:
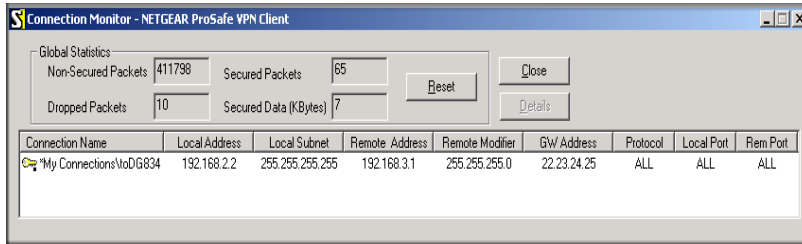

Figure 6-18

In this example you can see these settings:

- The DG834G v4 has a GW Address (public IP WAN address) of 22.23.24.25.
- The DG834G v4 has a Remote Address (LAN IP address) of 192.168.3.1.
- The VPN client PC has a Local Address (dynamically assigned address) of 192.168.2.2.

While the connection is being established, the **Connection Name** field in this screen displays **SA** before the name of the connection. When the connection is successful, the **SA** changes to the yellow key symbol shown in the previous figure.

> **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 must close the VPN connection to have normal Internet access.

Setting Up a Gateway-to-Gateway VPN Configuration

> → **Note:** This section describes how to use 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 "Setting Up VPN Tunnels in Special Circumstances" on page 6-32 for information about how to set up the VPN tunnel.

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

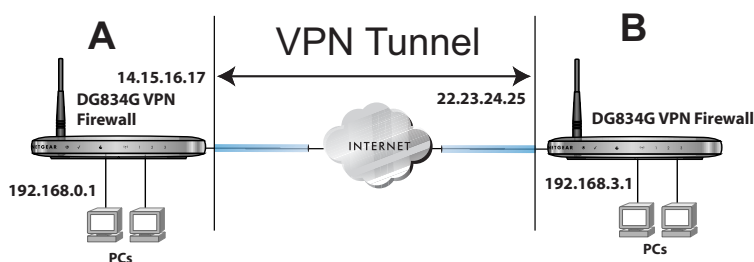**Figure 6-19**

v2.0, September 2007

Set the LAN IPs on each DG834G v4 to different subnets and configure each properly for the Internet. The examples below assume the following settings:

Table 6-4.   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)**
VPN Endpoint	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
DG834G v4_A	**GW_A**	**192.168.0.1**	**255.255.255.0**	**14.15.16.17**
DG834G v4_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.

To configure a gateway-to-gateway VPN tunnel using the VPN Wizard:

1. Log in to the DG834G v4 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**. Select VPN Wizard on the main menu. The VPN Wizard screen displays:
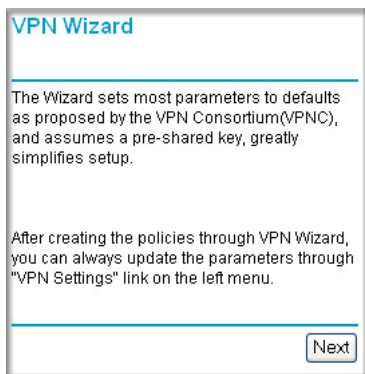

Figure 6-20

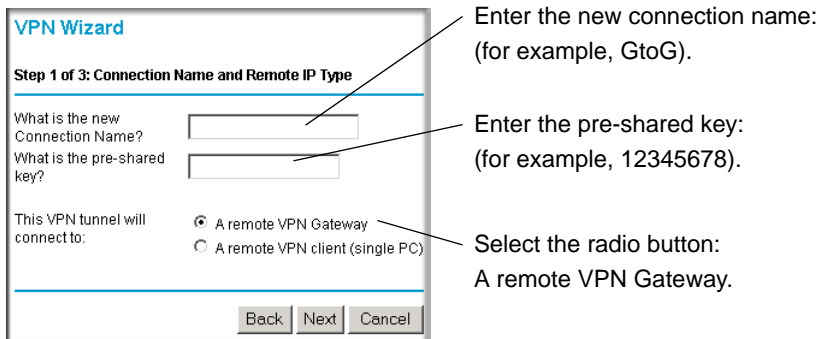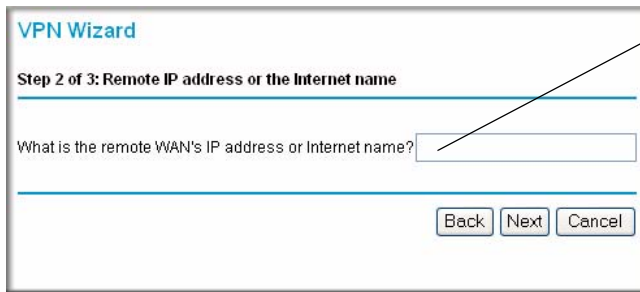2. Click **Next** to proceed, and the Step 1 of 3 screen displays:

Figure 6-21

3. Fill in the connection name and pre-shared key fields. Select the radio button for the type of target end point, and then click **Next** to proceed. The Step 2 of 3 screen displays:
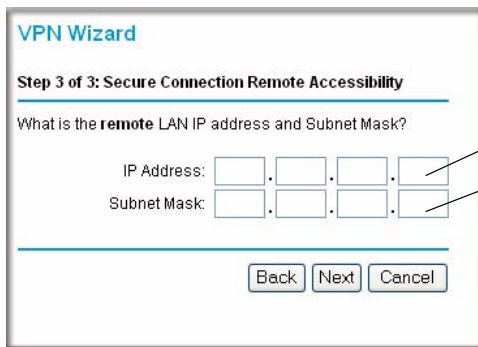
VPN Wizard

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

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

[Back] [Next] [Cancel]

Enter the WAN IP address of the remote VPN gateway: (for example, 22.23.24.25)

Figure 6-22

4. Fill in the IP address or FQDN for the target VPN endpoint WAN connection, and then click **Next**. The Step 3 of 3 screen displays:

VPN Wizard

Step 3 of 3: Secure Connection Remote Accessibility

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

IP Address: ___ . ___ . ___ . ___
Subnet Mask: ___ . ___ . ___ . ___

[Back] [Next] [Cancel]

Enter the LAN IP settings of the remote VPN gateway:

- IP Address (for example, 192.168.3.1)
- Subnet Mask (for example, 255.255.255.0)

Figure 6-23

5. Fill in the **IP Address** and **Subnet Mask** fields for the target endpoint that can use this tunnel, and then click **Next**.

The VPN Wizard Summary screen displays:

Figure 6-24

To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the **here** link (see Figure 6-24). You can click **Back** to return to the Summary screen.

Figure 6-25

6. Click **Done** on the Summary screen (see Figure 6-24) to complete the configuration procedure. The VPN Policies screen displays, showing that the new tunnel is enabled.

VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	ESP
⦿	1	☑	GtoG	Auto	192.168.0.1 / 255.255.255.0	192.168.3.1 / 255.255.255.0	3DES

Edit   Delete

Apply   Cancel

Add Auto Policy   Add Manual Policy

Figure 6-26

➡️ **Note:** See "Using Auto Policy to Configure VPN Tunnels" on page 6-32 for information about how to enable the IKE keepalive capability on an existing VPN tunnel.

7. Repeat these steps for the DG834G v4 on LAN B, and pay special attention to using the following network settings:

- WAN IP of the remote VPN gateway (for example, **14.15.16.17**)
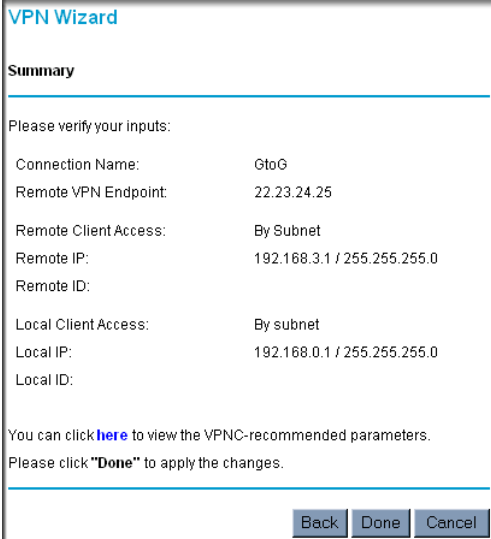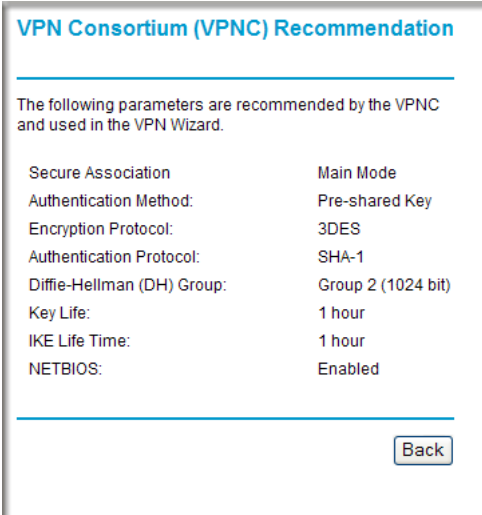- LAN IP settings of the remote VPN gateway:
    - IP Address (for example, **192.168.0.1**)
    - Subnet Mask (for example, **255.255.255.0**)
    - Preshared Key (for example, **12345678**)

8. 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 6-25 for information about the other ways.

    a. On the DG834G v4 main menu, select VPN Status. The VPN Status/Log screen displays:

VPN Status/Log

```
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
```

Refresh   Clear Log   VPN Status

Figure 6-27

    b. Click the **VPN Status** button to get the Current VPN Tunnels (SAs) screen:

Current VPN Tunnels (SAs) - Microsoft Internet Explorer

Current VPN Tunnels (SAs)

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
2	---	---	GtoG	---	Connect	---	---
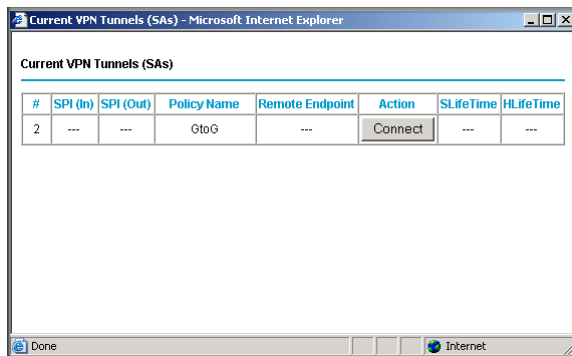
Figure 6-28

    c. Click **Connect** for the VPN tunnel you want to activate. View the VPN Status/Log screen (Figure 6-29) 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 screen.
- Activate the VPN tunnel by pinging the remote endpoint.
- Start using the VPN tunnel.

> **Note:** See "Using Auto Policy to Configure VPN Tunnels" on page 6-32 for information about how 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:

1. Log in to the modem router.

2. On the main menu, select VPN Status. The VPN Status/Log screen displays:

VPN Status/Log

```
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
```
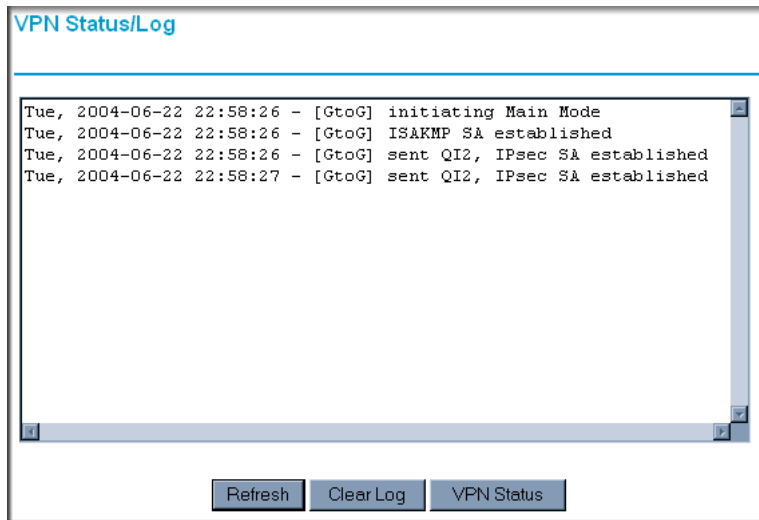
Refresh   Clear Log   VPN Status
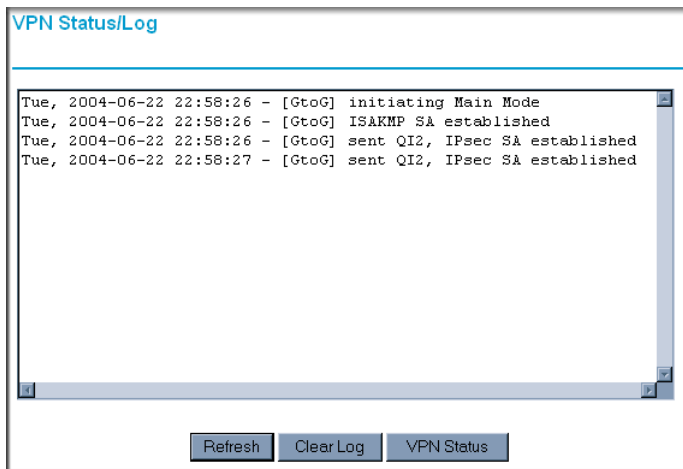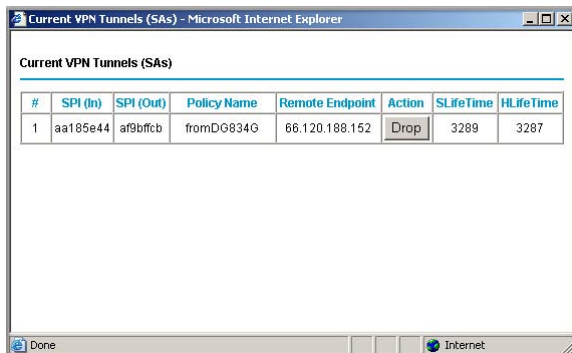
Figure 6-29

3. Click **VPN Status** to get the Current VPN Tunnels (SAs) screen:

Figure 6-30

4. Click **Connect** for the VPN tunnel that you want to activate.

Activating 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 (for example, 192.168.3.1), perform 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 DG834G v4's network by using the Connect option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client reports 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**.
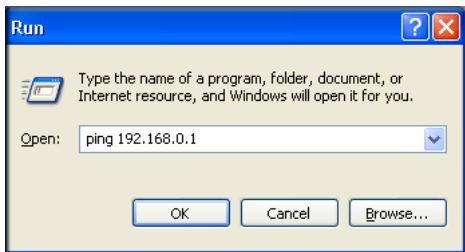
Running a ping test
to the LAN from the PC

Figure 6-31

This causes a continuous ping to be sent to the first DG834G v4. Within two minutes, the
ping response should change from timed out to reply.

→ **Note:** You can 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 6-32

Once the connection is established, you can open a browser on the PC and enter the LAN IP
address of the remote DG834G v4. After a short wait, you should see the login screen of the
modem router (unless another PC already has the DG834G v4 management interface open).

• **Gateway-to-gateway configuration**. Test the VPN tunnel by pinging the remote network
from a PC attached to the DG834G v4.

a. Open a command prompt (for example, Start > Run > cmd).

b. Type **ping 192.168.3.1**.

Figure 6-33

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

Start Using a VPN Tunnel to Activate 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 screen to determine the status of a VPN tunnel:

1. Log in to the modem router.

2. On the main menu, select VPN Status to display the VPN Status/Log screen.
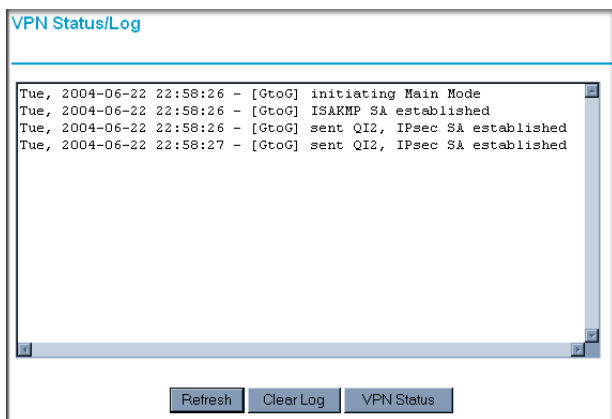
Figure 6-34

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.

3. On the VPN Status/Log screen, click **VPN Status** to display the Current VPN Tunnels (SAs) screen.

Figure 6-35

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 VPN policy associated with this SA.

• **Remote Endpoint**. The IP address on the remote VPN endpoint.

• **Action**. Either a **Drop** or a **Connect** button.

• **SLifeTime (Secs)**. The remaining soft lifetime for this SA in seconds. When the soft lifetime becomes 0 (zero), the SA (Security Association) is re-negotiated.

• **HLifeTime (Secs)**. The remaining hard lifetime for this SA in seconds. When the hard lifetime becomes 0 (zero), the SA (Security Association) is terminated. (It is re-established if required.)

Deactivating a VPN Tunnel
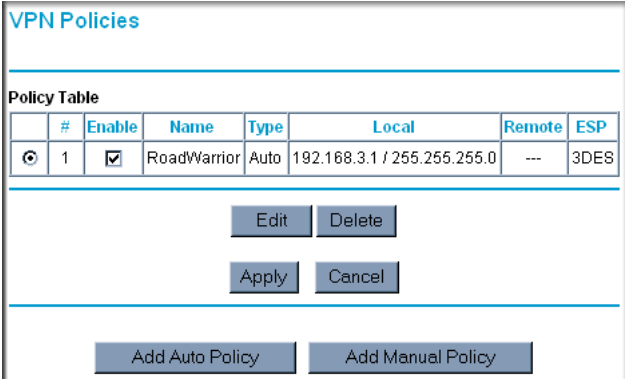
Sometimes a VPN tunnel must be deactivated for testing purposes. You can deactivate a VPN tunnel from two places:

• Policy table on VPN Policies screen
• VPN Status screen

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

To use the VPN Policies screen to deactivate a VPN tunnel:

1. Log in to the modem router.

2. On the main menu, select VPN Policies to display the VPN Policies screen.

Figure 6-36

3. In the Policy Table, clear the **Enable** check box for the VPN tunnel that you want to deactivate, and then click **Apply**. (To reactivate the tunnel, select the **Enable** check box, and then click **Apply**.)

Using the VPN Status Screen to Deactivate a VPN Tunnel

To use the VPN Status screen to deactivate a VPN tunnel:

1. Log in to the modem router.

2. On the main menu, select VPN Policies to display the VPN Policies screen.

VPN Status/Log

```
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
```

Refresh   Clear Log   VPN Status

Figure 6-37

3. Click **VPN Status**. The Current VPN Tunnels (SAs) screen displays:

Current VPN Tunnels (SAs) - Microsoft Internet Explorer

Current VPN Tunnels (SAs)

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

Done   Internet

Figure 6-38

4. Click **Drop** for the VPN tunnel that you want to deactivate.

Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the modem router.

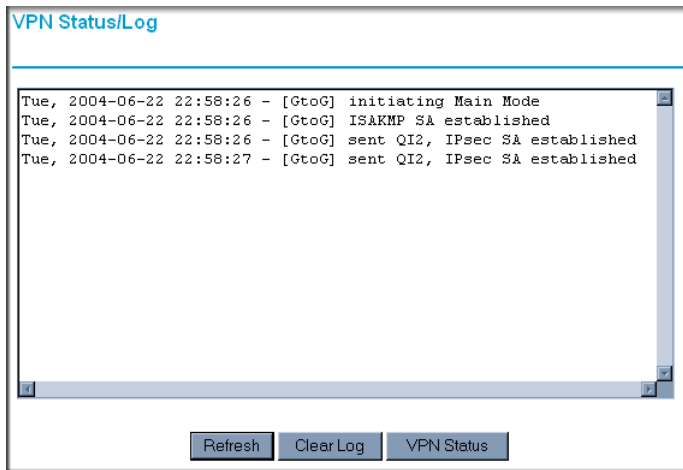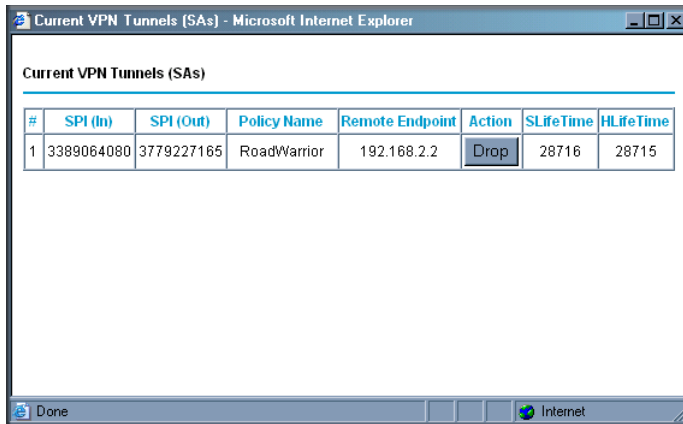**2.** On the main menu, select VPN Policies to display the VPN Policies screen. In the Policy Table, select the radio button for the VPN tunnel to be deleted, and then click **Delete**.

Figure 6-39

Setting Up VPN Tunnels in Special Circumstances

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

*   **Auto Policy**. For a typical automated Internet Key Exchange (IKE) setup, see "Using Auto Policy to Configure VPN Tunnels" on page 6-32. 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 6-41. 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 DG834G v4 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 6-37 for an example of using Auto Policy.

Configuring VPN Network Connection Parameters

All VPN tunnels on the modem router requires taht you configure 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.

Select VPN Policies on the main menu, and then click the **Add Auto Policy** button to display the VPN - Auto Policy screen:

Figure 6-40

The DG834G v4 VPN tunnel network connection fields are defined in the following table.

Table 6-5.   VPN-Auto Policy Screen Settings

Fields and Settings		Description
General	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	• The remote VPN endpoint must have this VPN gateway's address entered as its 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 an option (IP address or domain name) and enter the address of the remote VPN endpoint to which you want to connect.
	IKE Keep-alive.	• If you want to ensure that a connection is kept open, or, if that is not possible, that it is quickly re-established when disconnected, select this check box. • 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 The remote VPN endpoint must have these IP addresses entered as its remote addresses.	Subnet Mask	Enter the desired network mask.
	Single/Start IP Address	• Enter the IP address for a single address, or the starting address for an address range. A single adress setting is used when you want to make a single server on your LAN available to remote users. A range must be an address range used on your LAN. • **Any**. The remote VPN endpoint may be at any IP address.
	Finish IP Address	For an address range, enter the finish IP address. This must be an address range used on your LAN.

Table 6-5.   VPN-Auto Policy Screen Settings (continued)

Fields and Settings		Description
Remote LAN The remote VPN endpoint must have these IP addresses entered as its Local addresses.	IP Address	**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/Start IP Address	• Enter an IP address that is on the remote LAN. You can use this setting when you want to access a server on the remote LAN. • For a range of addresses, enter the starting IP address. This must be an address range used on the remote LAN. • **Any**. Any outgoing traffic from the **Local IP** computers will trigger an attempted VPN connection to the remote VPN endpoint. Please be sure you want this option before selecting it.
	Finish IP Address	Enter the finish IP address for a range of addresses. This must be an address range used on the remote LAN.
	Subnet Mask	Enter the network mask.
IKE	Direction	This setting is used when determining if the IKE policy matches the current traffic. Select an option. • **Responder only**. Incoming connections are allowed, but outgoing connections are blocked. • **Initiator and Responder**. Both incoming and outgoing connections are allowed.
	Exchange Mode	Ensure that 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 an 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 local identity type that you selected. (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 Nam**e. 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 remote identity type that you selected. If **IP Address** is selected, no input is required.

Table 6-5. VPN-Auto Policy Screen Settings (continued)

Fields and Settings		Description
Parameters	Encryption Algorithm	The 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	The 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. This is the default.
	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.
	Enable IPSec PFS (Perfect Forward Secrecy)	• If this check box is selected, 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 might 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.

Virtual Private Networking

Example of Using Auto Policy
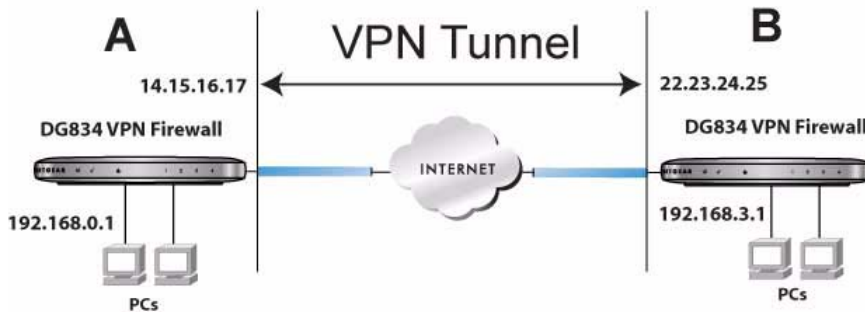
Figure 6-41

To use Autho Policy:

1. Set the LAN IPs on each DG834G v4 modem router to different subnets and configure each properly for the Internet. The following settings are assumed for this example:

Table 6-6. 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)**
VPN Endpoint	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
DG834G v4 A	**LAN_A**	**192.168.0.1**	**255.255.255.0**	**14.15.16.17**
DG834G v4 B	**LAN_B**	**192.168.3.1**	**255.255.255.0**	**22.23.24.25**

2. On the main menu, select VPN Policies to display the VPN Policies screen:

Figure 6-42

3. Click **Add Auto Policy**. The VPN Auto Policy screen displays:

Figure 6-43

4. Enter these policy settings:

Auto Policy Field		Setting
General	Policy Name	GtoG
	Remote VPN Endpoint Address Type	Fixed
	Remote VPN Endpoint Address Data	22.23.24.25
Local LAN		Use the default settings.
Remote LAN	IP Address	Select **Subnet address** from the drop-down list.
	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 the default setting.
	Remote Identity Type	Use the default setting.
Parameters	Encryption Algorithm	3DES
	Authentication Algorithm	MD5
	Pre-shared Key	12345678

5. Click **Apply**. The VPN Policies screen displays:

Figure 6-44

6. Repeat these steps for the DG834G v4 on LAN B. Pay special attention to the following network settings:

- General, Remote Address Data (for example, **14.15.16.17**)
- Remote LAN, Start IP Address
    - IP Address (for example, **192.168.0.1**)
    - Subnet Mask (for example, **255.255.255.0**)
    - Pre-shared Key (for example, **12345678**)

7. Use the VPN Status screen to activate the VPN tunnel:

> → **Note:** The VPN Status screen is only one of three ways to active a VPN tunnel. See "Activating a VPN Tunnel" on page 6-25 for information about the other ways.

a. From the main menu, select VPN Status to display the VPN Status/Log screen. Then click **VPN Status** to display the Current VPN Tunnels (SAs) screen:
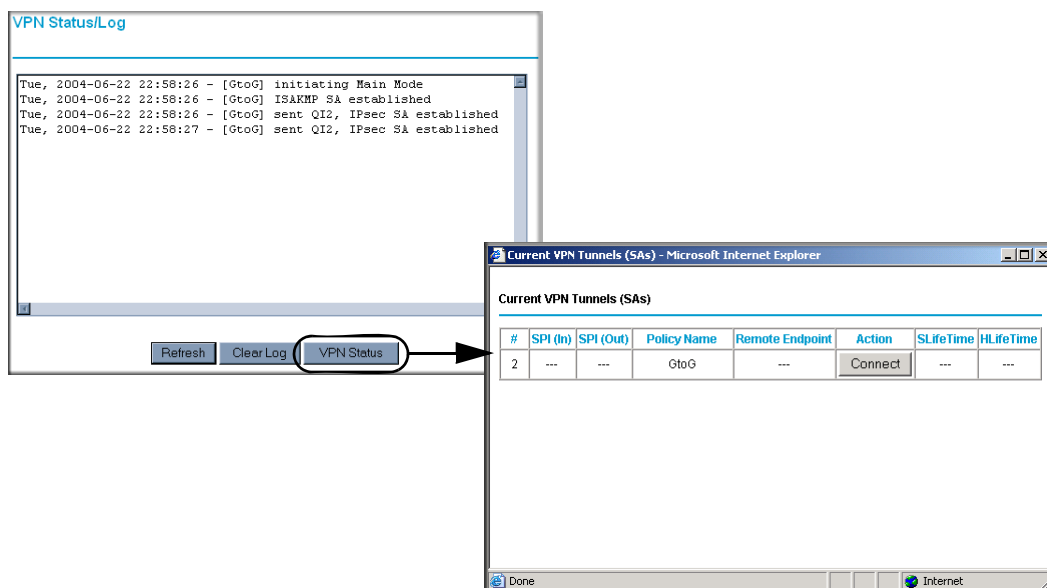
Figure 6-45

b. Click **Connect** for the VPN tunnel that you want to activate. Review the VPN Status/Log screen (Figure 6-45) 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).

On the main menu, select VPN Policies, and then click the **Add Manual Policy** radio button to display the VPN - Manual Policy screen:

Figure 6-46

The following table explains the fields in the VPN Manual Policy screen.

Table 6-7.   VPN Manual Policy Fields and Settings

Fields and Settings		Description
General The DG834G v4 VPN tunnel network connection fields.	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	• The remote VPN endpoint must have this VPN gateway's address entered as its 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 an option (IP address or domain name) and enter the address of the remote VPN endpoint to which you want to connect.
Local LAN The remote VPN endpoint must have these IP addresses entered as its remote addresses.	Subnet Mask	Enter the network mask.
	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/Start IP Address	• Enter the IP address for a single address, or the starting address for an address range. A single adress setting is used when you want to make a single server on your LAN available to remote users. A range must be an address range used on your LAN. • **Any**. The remote VPN endpoint may be at any IP address.
	Finish IP Address	For an address range, enter the finish IP address. This must be an address range used on your LAN.

Table 6-7. VPN Manual Policy Fields and Settings (continued)

Fields and Settings		Description
Remote LAN The remote VPN endpoint must have these IP addresses entered as its Local addresses.	IP Address	**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/Start IP Address	• Enter an IP address that is on the remote LAN. You can use this setting when you want to access a server on the remote LAN. • For a range of addresses, enter the starting IP address. This must be an address range used on the remote LAN. • **Any**. Any outgoing traffic from the **Local IP** computers will trigger an attempted VPN connection to the remote VPN endpoint. Please be sure you want this option before selecting it.
	Finish IP Address	Enter the finish IP address for a range of addresses. This must be an address range used on the remote LAN.
	Subnet Mask	Enter the network mask.
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 an 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 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 ADSL2+ Modem Wireless 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 Access to the Modem Router Main Menu" 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 7-8.

- I want to clear the configuration and start over again.

    Go to "Restoring the Default Configuration and Password" on page 7-8.

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.

2. After approximately 10 seconds, verify that:

    a. The Power LED is still solid green. A red light indicates the unit has failed its power-on self-test (POST).

   b.   The Ethernet LAN port LEDs are lit for any local ports that are connected.

   If a LAN 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 is amber.

   c.   The DSL and Internet LEDs are lit.

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

Power LED Is 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 12V DC power adapter supplied by NETGEAR for this product.

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

Power LED Is Red

When the router is turned on, the modem router performs a power-on self-test. If the the Power LED turns red, there is a fault within the router. Try to clear the fault as follows:

*   Cycle the power to see if the router recovers.

*   Clear the router's configuration to factory defaults. This sets 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 DSL or Internet Port LEDs Are Not On

If these LEDs 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 that you are using the correct cable. When connecting the router's WAN ADSL port, use the cable that was supplied with the DG834G v4.

Troubleshooting Access to the Modem Router Main Menu

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the 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. See the online document listed in "Preparing a Computer for Network Access" in Appendix C to find your computer's IP address.

> **Note:** If your computer's IP address is shown as 169.254.x.x:
> Recent versions of Windows and MacOS 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 that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that 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 screen or tab, or your changes are lost.

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

Troubleshooting the ISP Connection

ADSL Link

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

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 DSL LED.

DSL LED Is Solid Green

If your DSL LED is solid 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.

DSL LED Is Blinking

If your DSL LED is blinking, then your modem router is attempting to make an ADSL connection with the service provider. The LED should turn solid green within a few minutes.

If the DSL LED does not turn solid 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 solid green DSL 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.

DSL LED Is Off

If the DSL 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 solid green DSL 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 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, determine whether the modem router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your modem router must request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

To check the WAN IP address from the browser interface:

1. Launch your browser, and select an external site such as www.netgear.com.

2. Access the modem router main menu 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 might be one of the following:

• Your ISP might require a multiplexing method or virtual path identifier or virtual channel identifier parameter.
  Verify with your ISP the multiplexing method and parameter value, and update the router's ADSL settings accordingly.

• Your ISP might 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, the service name, user name, and password might be set incorrectly. See "Troubleshooting PPPoE or PPPoA", below.

• Your ISP might 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 might check for your computer's MAC address. In this case try either of the following:

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

– Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings screen.

Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

1. Access the main menu of the router at **http://192.168.0.1**.

2. Under the Maintenance heading, select Router Status.

3. Click **Connection Status**.

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, the service name, user name, or password might be incorrect. There also might 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 might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the 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 might 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 the link to the online document "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 PC 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 working correctly, you could have one of the following problems:

   • Wrong physical connections

   – Make sure that the LAN port LED is on. If the LED is off, follow the instructions in "LAN or DSL or Internet Port LEDs Are 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.

v2.0, September 2007

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.

1. From the Windows toolbar, click the **Start** button, and select **Run**.

2. In the Windows Run window, type:

PING -n 10 *IP address*

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

If the path is functioning correctly, replies 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 isnot 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 the online document listed 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 screen.

• Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing only 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. See the *ADSL2+ Modem Wirelesss Router Setup Manual*.

Restoring the Default Configuration and Password

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

• Use the Erase function (see "Backing Up, Restoring, or Erasing Your Settings" on page 4-1).

• Use the 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 reset button on the rear panel of the router.

1. Press and hold the reset button until the Power LED turns red (about 6 seconds).

2. Release the reset button and wait for the router to reboot.

Problems with Date and Time

The E-mail screen in the Content Filtering section displays the current date and time of day. The ADSL2+ Modem Wireless Router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

• Date shown is January 1, 2000.
  Cause: The 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 5 minutes, and check the date and time again.

• Time is off by one hour.
  Cause: The router does not automatically sense daylight savings time. On the E-mail screen, select or clear the **Adjust for Daylight Savings Time** check box.

v2.0, September 2007

Appendix A
Technical Specifications

This appendix provides technical specifications for the 54 Mbps ADSL2+ Modem Wireless Router Model DG834G.

Network Protocol and Standards Compatibility		
	Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPPoA, or PPTP, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power Adapter		
	North America:	120V AC, 60 Hz, input
	United Kingdom, Australia:	240V AC, 50 Hz, input
	Europe:	230V AC, 50 Hz, input
	Japan:	100V AC, 50/60 Hz, input
	All regions (output):	12 V DC @ 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 (32º to 104º 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 (for the DG834G) or ITU Annex B (for the DG834GB)

Technical Specifications

NETGEAR VPN Configuration

DG834G v4 to FVL328

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DG834G v4 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 that the firmware is up to date, and taht you have all 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
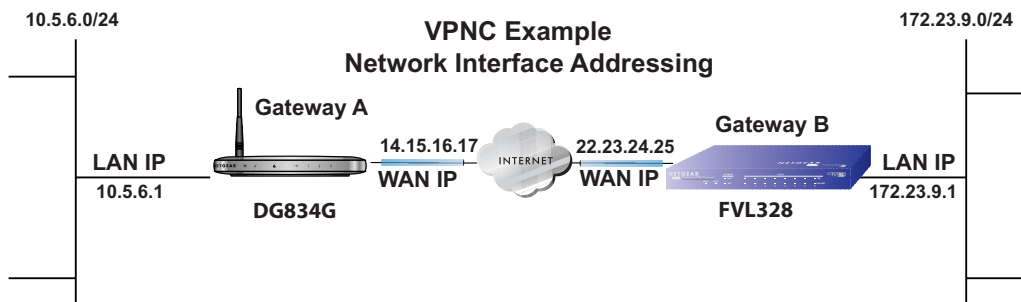
Figure B-1

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

Step-By-Step Configuration

1. Configure the DG834G v4 as in the gateway-to-gateway procedures using the VPN Wizard (see "Setting Up a Gateway-to-Gateway VPN Configuration" on page 6-18), being certain to use appropriate network addresses for the environment.

The LAN addresses used in this example are as follows:

Unit	WAN IP	LAN IP	LAN Subnet Mask
DG834G	14.15.16.17	10.5.6.1	255.255.255.0
FVL328	22.13.24.25	172.23.9.1	255.255.255.0

    a. Enter **toFVL328** for the connection name.

    b. Enter **22.23.24.25** for the remote WAN's IP address.

    c. Enter the following:

        • IP Address: **172.23.9.1**

        • Subnet Mask: **255.255.255.0**

Click VPN Policies under
the Advanced - VPN heading to display
this screen.

Figure B-2

2. Configure the FVL328 as in the gateway-to-gateway procedures for the VPN Wizard (see "Setting Up a Gateway-to-Gateway VPN Configuration" on page 6-18), being certain to use appropriate network addresses for the environment.

    a. Enter **toDG834** for the connection name

    b. Enter **14.15.16.17** for the remote WAN's IP address

    c. Enter the following:

       • IP Address: **10.5.6.1**

       • Subnet Mask: **255.255.255.0**

Select IKE Policies under the VPN heading
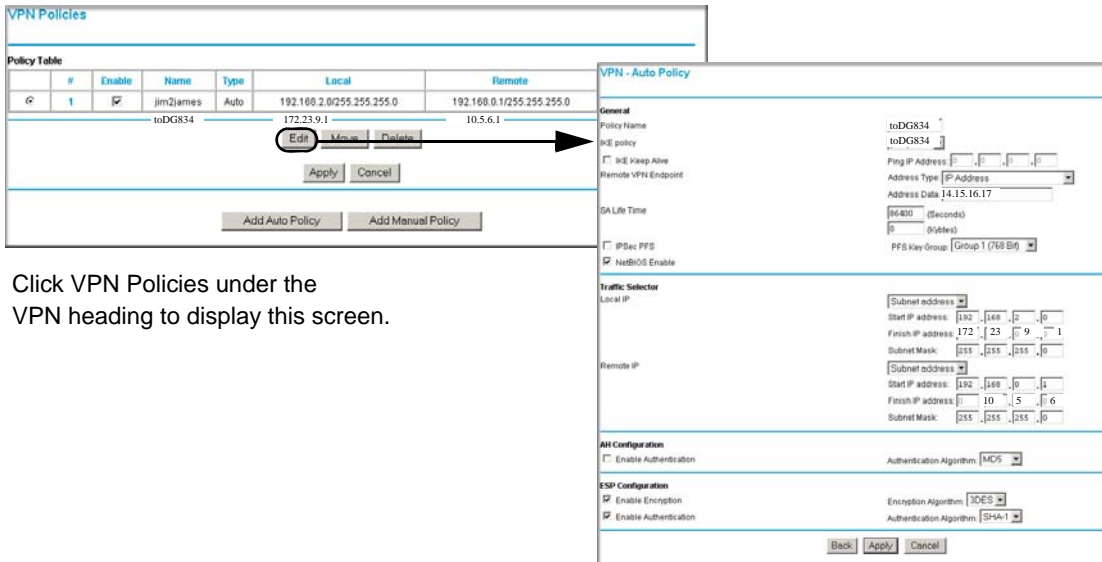to display the IKE Policy Configuration screen.
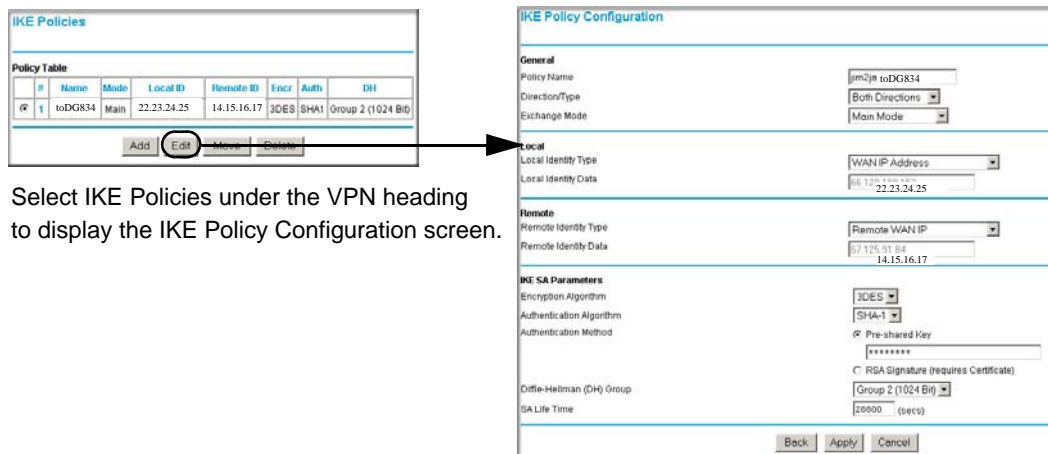
Figure B-3

Click VPN Policies under the
VPN heading to display this screen.

Figure B-4

3. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834G v4.

   a. Open the command prompt (Start > Run > cmd)
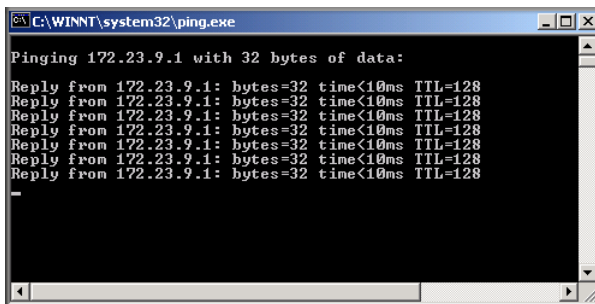
   b. Type **ping 172.23.9**.1

Figure B-5

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

DG834G v4 with FQDN to FVL328

This section is a case study on how to configure a VPN tunnel from a NETGEAR DG834G v4 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 section follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify that the firmware is up to date, and that you have all 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-2. Profile Summary

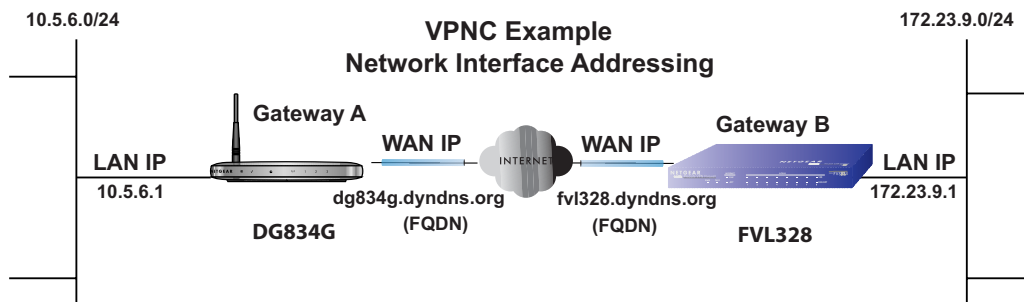| VPN Consortium Scenario:	Scenario 1	
Type of VPN	LAN-to-LAN or Gateway-to-Gateway (not PC/Client-to-Gateway)	
Security Scheme:	IKE with Preshared Secret/Key (not Certificate-based)	
IP Addressing:		
	NETGEAR-Gateway A	Fully Qualified Domain Name (FQDN)
	NETGEAR-Gateway B	FDQN

Figure B-6

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

Using 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 e-mail addresses, host names, and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a third-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. Some 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 **dg834g.dyndns.org** for Gateway A using the DynDNS service. Gateway B uses the DDNS service provider when establishing a VPN tunnel.

To establish VPN connectivity, Gateway A must be configured to use Dynamic DNS, and Gateway B must be configured to use a DNS host name provided by a DDNS service provider to find Gateway A. 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 DG834G v4 labeled Gateway A as in the illustration.

   Out of the box, the DG834G v4 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**. This example assumes that you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. On the DG834G v4, configure the Dynamic DNS settings.

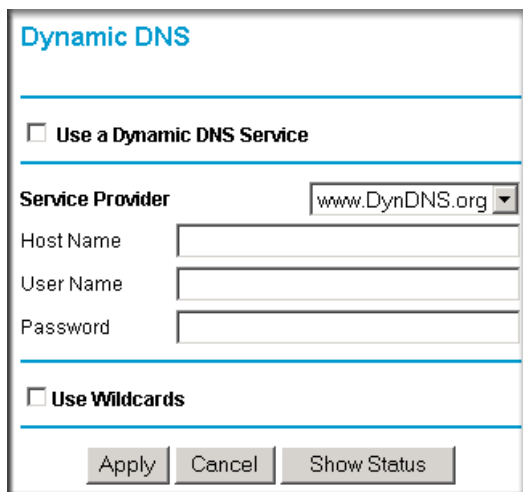**a.** Under the Advanced Heading, select Dyanmic DNS to display the Dynamic DNS Setup screen:

Figure B-7

b. Configure this screen with appropriate account and hostname settings and then click **Apply**.

- Select the **Use a Dynamic DNS Service** check box.
- In the **Host Name** field type d**g834g.dyndns.org**.
- In the **User Name** field enter the account user name.
- In the **Password** field enter the account password.

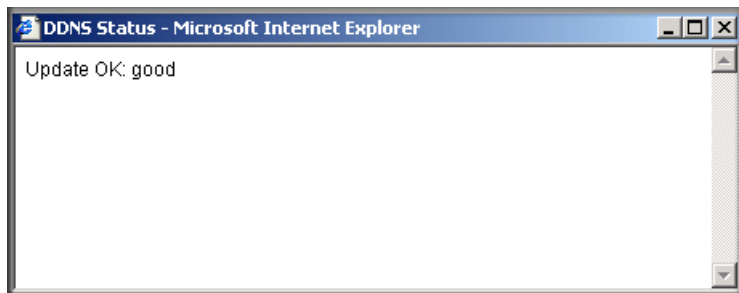**c.** Click **Show Status**. The resulting screen should show Update OK: good:

Figure B-8

3. On the FVL328, configure the Dynamic DNS settings. Assume a correctly configured DynDNS account.

    a. From the main menu, select Dynamic DNS to display the Dynamic DNS Setup screen:
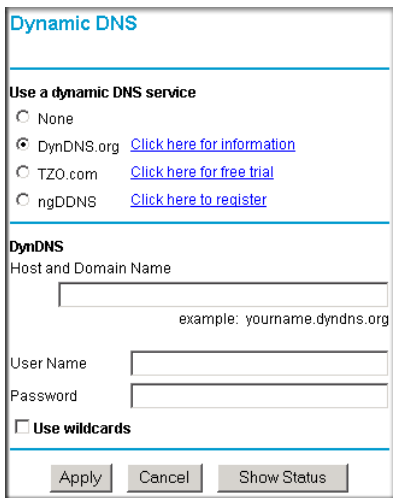
Figure B-9

    b. Select the **DynDNS.org** radio button. The Dynamic DNS screen displays:

Figure B-10

    c. Configure the appropriate account and host name settings, and then click **Apply**.

       • In the **Host and Domain Name** field enter **fvl328.dyndns.org**.

       • In the **User Name** field enter the account user name.

       • In the **Password** field enter the account password.

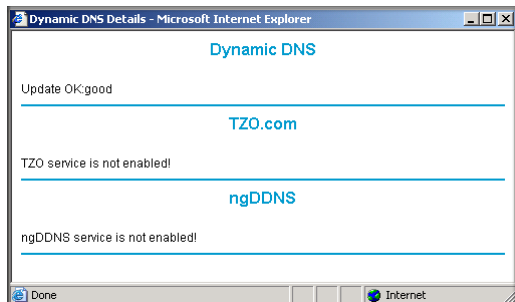**d.** Click **Show Status**. The resulting screen should show `Update OK: good:`

Figure B-11

4. Configure the DG834G v4 as in the gateway-to-gateway procedures using the VPN Wizard (see "Setting Up a Gateway-to-Gateway VPN Configuration" on page 6-18), being certain to use appropriate network addresses for the environment.

The LAN addresses used in this example are as follows:1

Device	LAN IP Address	LAN Subnet Mask
DG834G v4	10.5.6.1	255.255.255.0
FVL328	172.23.6.1	255.255.255.0

a. Enter **toFVL328** for the connection name.

b. Enter **fvl328.dyndns.org** for the remote WAN's IP address.

c. Enter the following:
- IP Address: **172.23.9.1**
- Subnet Mask: **255.255.255.0**

5. Configure the FVL328 as in the gateway-to-gateway procedures for the VPN Wizard (see "Setting Up a Gateway-to-Gateway VPN Configuration" on page 6-18), being certain to use appropriate network addresses for the environment.

a. Enter **toDG834** for the Connection Name.

b. Enter **dg834g.dyndns.org** for the remote WAN's IP address.

c. Enter the following:
- IP Address: **10.5.6.1**
- Subnet Mask: **255.255.255.0**

6. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834G v4.

    a. Open the command prompt (Start -> Run -> cmd)
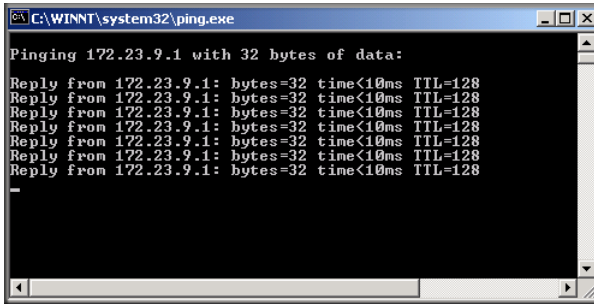
    b. Type **ping 172.23.9.1**

Figure B-12

> → **Note:** The pings might fail the first time. If this happens, try the pings a second time.

Configuration Summary (Telecommuter Example)

The configuration in this section 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-3. Configuration Summary (Telecommuter Example)

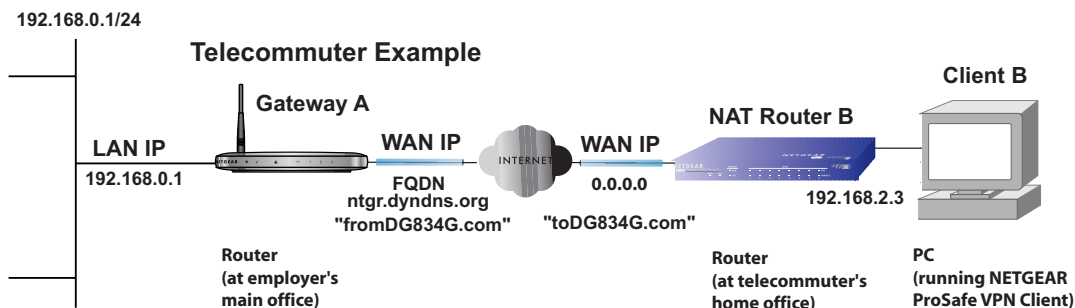| VPN Consortium Scenario:		Scenario 1
Type of VPN:		PC/client-to-gateway, with client behind NAT router
Security Scheme:		IKE with Pre-shared Secret/Key (not certificate-based)
IP Addressing:		
	Gateway	Fully Qualified Domain Name (FQDN)
	Client	Dynamic

Figure B-13

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 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**. Select **VPN Policies** to display the VPN Policies screen. Click **Add Auto Policy** to proceed and enter the information.

VPN - Auto Policy

General

Policy Name	fromDG834G	← **fromDG834G** (in the example)
Remote VPN Endpoint	Address Type: Dynamic IP address ←	**Dynamic IP address**
	Address Data: n/a	

☑ NetBIOS Enable

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

IKE Keep Alive is optional; must match
Remote LAN IP Address when enabled
(remote PC must respond to pings)

Local LAN

IP Address	Subnet address ←	**Subnet address**
	Single/Start address: 192 . 168 . 0 . 1 ←	**192.168.0.1** (in this example)
	Finish address:	
	Subnet Mask: 255 . 255 . 255 . 0 ←	**255.255.255.0**

Remote LAN

IP Address	Single address ←	**Single address**
	Single/Start IP address: 192 . 168 . 2 . 3 ←	**192.168.2.3** (in this example)
	Finish IP address:	(Remote NAT router must have
	Subnet Mask:	**Address Reservation** set and

VPN Passthrough enabled)

IKE

Direction	Responder only	
Exchange Mode	Main Mode ←	**Main Mode**
Diffie-Hellman (DH) Group	Auto	
Local Identity Type	Fully Qualified Domain Name ←	**Fully Qualified Domain Name**
Data	fromDG834G.com ←	**fromDG834G.com** (in this example)
Remote Identity Type	Fully Qualified Domain Name ←	**Fully Qualified Domain Name**
Data	toDG834G.com ←	**toDG834G.com** (in this example)

Parameters

Encryption Algorithm	3DES ←	**3DES**
Authentication Algorithm	Auto	
Pre-shared Key	12345678 ←	**12345678** (in this example)
SA Life Time	3600 (seconds) ←	**3600**

☐ Enable PFS (Perfect Forward Security)

[Back] [Apply] [Cancel]

Figure B-14

2. Click **Apply** when you are finished to display the VPN Policies screen.

Figure B-15

To view or modify the tunnel settings, select the radio button next to the tunnel entry, and then 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 ADSL2+ Modem Wireless Router. This procedure assumes that 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*) for information about how to purchase the NETGEAR ProSafe VPN Client.

> → **Note:** Before installing the ADSL2+ Modem Wireless Router software, be sure to turn off any virus protection or firewall software you might be running on your PC.

1. Install the NETGEA ProSafe VPN Client on the remote PC, and then reboot.

    a. You might 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 might 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 might 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 (![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**, and then click **Connection**. A New Connection listing appears in the list of policies. Rename the new connection so that it matches the connection name that you entered in the VPN settings of the DG834G v4 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-17) because connection names are irrelevant to how the VPN tunnel functions.

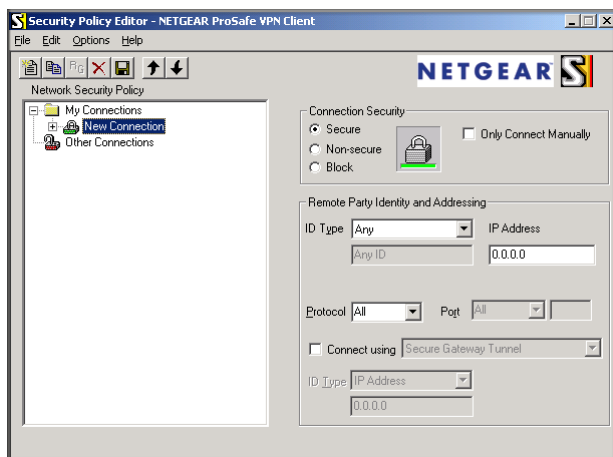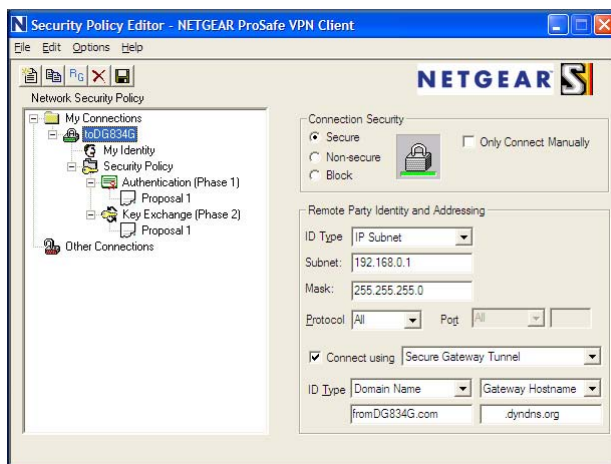> 💡 **Tip:** Choose connection names that make sense to the people using and administrating the VPN.

Figure B-16

Figure B-17

c. Select **Secure** in the **Connection Security** check-box group.

d. Select **IP Subnet** in the **ID Type** drop-down list.

e. In this example, type **192.168.0.1** in the **Subnet** field as the network address of the DG834G v4.

f. Enter **255.255.255.0** in the **Mask** field as the **LAN Subnet Mask** of the DG834G v4.

g. Select **All** in the **Protocol** drop-down list 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** drop-down list, 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-17.

3. Configure the Security Policy in the ADSL2+ Modem Wireless 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 appear below the connection name.

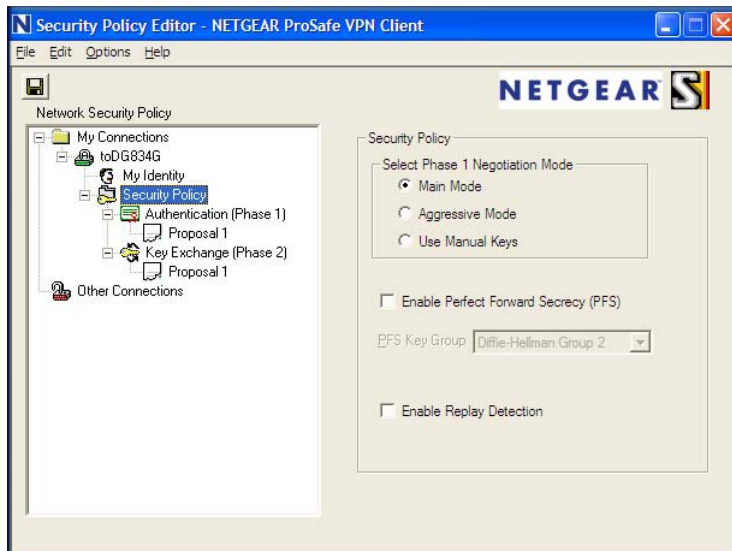**b.** Click Security Policy to show the Security Policy menu.

Figure B-18

c. Select the **Main Mode** radio button in the **Select Phase 1 Negotiation Mode** group.

4. Configure the VPN client identity.

In this step, you provide information about the remote VPN client PC. You must provide the pre-shared key that you configured in the DG834G v4 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**.
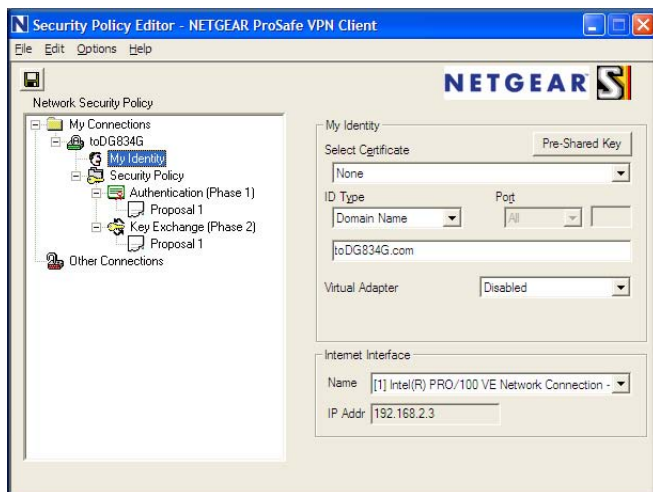

Figure B-19

b. Select **None** in the **Select Certificate** drop-down list.

c. Select **Domain Name** in the **ID Type** drop down list, and then enter **toDG834G.com** (in this example). Select **Disabled** in the **Virtual Adapter** drop-down list.

d. In the Internet Interface section, select **Intel PRO/100VE Network Connection** (in this example, your Ethernet adapter might be different) in the **Name** field, and then enter **192.168.2.3** (in this example) in the **IP Addr** field.
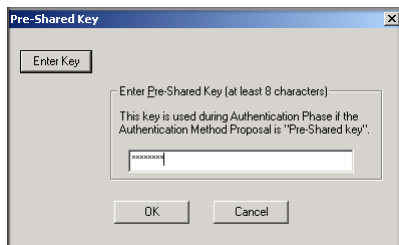
e. Click the **Pre-Shared Key** button.

Figure B-20

f. In the Pre-Shared Key screen, click **Enter Key**. Enter the DG834G v4's pre-shared key and click **OK**. In this example, **12345678** is entered. This field is case-sensitive.

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 the + symbol.

    b. Expand the Authentication subheading by double clicking its name or clicking the + symbol. Then select Proposal 1 below Authentication.
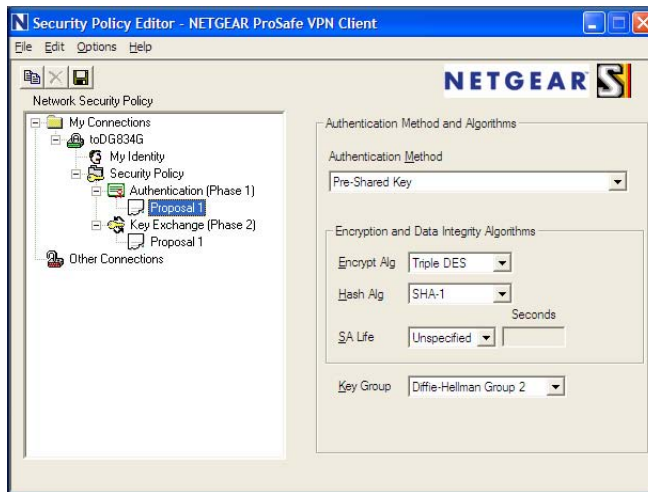

Figure B-21

    c. In the **Authentication Method** field, select **Pre-Shared Key**.

    d. In the **Encrypt Alg** drop-down list, select the type of encryption. In this example, use **Triple DES**.

    e. In the **Hash Alg** drop-down list, select **SHA-1**.

    f. In the **SA Life** drop-down list, select **Unspecified**.

    g. In the **Key Group** drop-down list, select **Diffie-Hellman Group 2**.

6. Configure the **VPN Client Key Exchange Proposal**.

In this step, you 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 the + symbol. Then select Proposal 1 below Key Exchange.
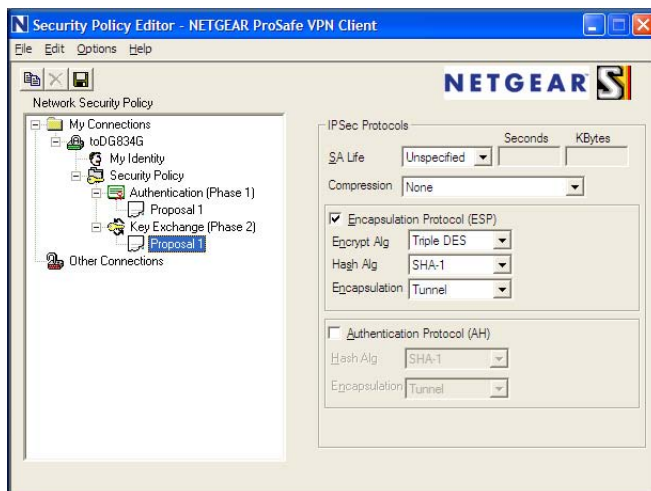

Figure B-22

b. In the **SA Life** drop-down list, select **Unspecified**.

c. In the **Compression** drop-down list, select **None**.

d. Select the **Encapsulation Protocol (ESP)** check box.

e. In the **Encrypt Alg** drop-down list, select the type of encryption. In this example, use **Triple DES**.

f. In the **Hash Alg** drop-down list, select **SHA-1**.

g. In the **Encapsulation** drop-down list, select **Tunnel**.

h. Leave the **Authentication Protocol (AH)** check box cleared.

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 automatically opens 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 modem router menu (see Figure B-23). 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. Select toDG834G.

The modem router reports the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.
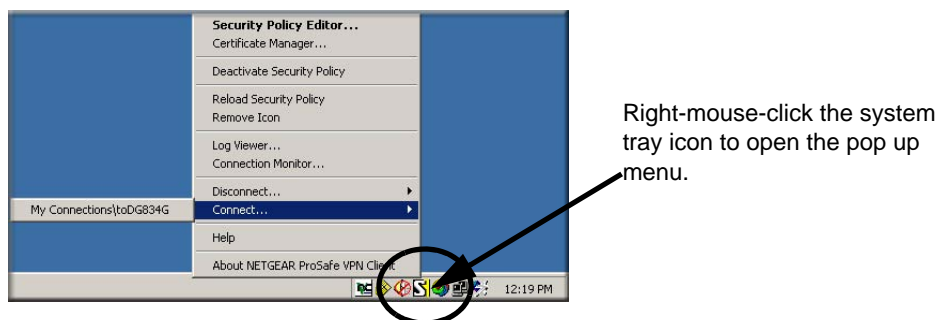

Right-mouse-click the system tray icon to open the pop up menu.

Figure B-23

To perform a ping test using this 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**.

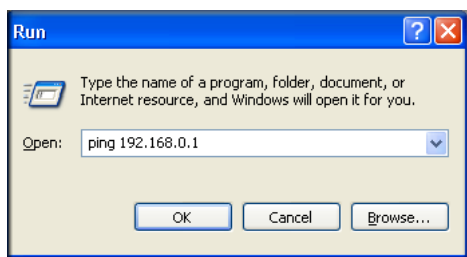**c.** Type **ping -t 192.168.0.1**, and then click **OK**.

Figure B-24

This causes a continuous ping to be sent to the VPN router. Within two minutes, the ping response should change from timed out to reply.

Figure B-25

Once the connection is established, you can open the browser on 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 diagnostics to test the VPN connection from the VPN router to the client PC. To do this, select Diagnostics on the modem 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 Log Viewer.

1. To launch this function, click the Windows **Start** button, then select Programs > 54 Mbps ADSL2+ Modem Wireless Router Model DG834G > 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.
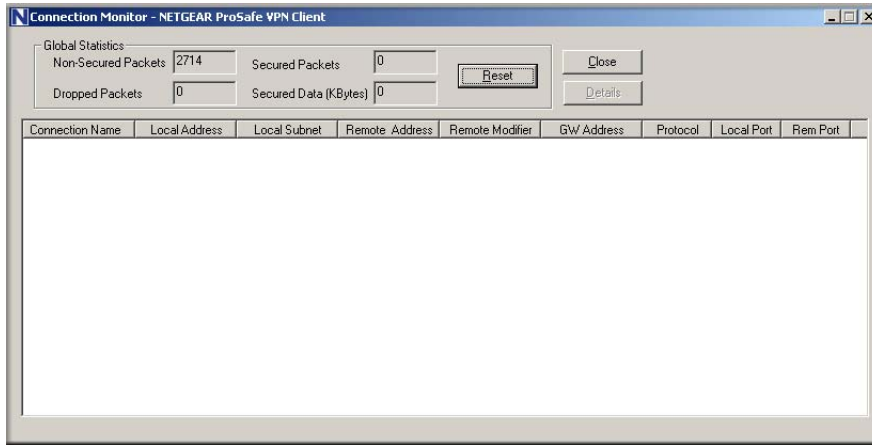
2. The Connection Monitor screen displays:

Figure B-26

While the connection is being established, the Connection Name listed in this screen shows SA before the name of the connection. When the connection is successful, the SA changes 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 to have normal Internet access.

Viewing the VPN Router's VPN Status and Log Information

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

1. On the modem router main menu, select Router Status, and then click the **VPN Status** button. The VPN Status/Log screen for a connection is shown below:
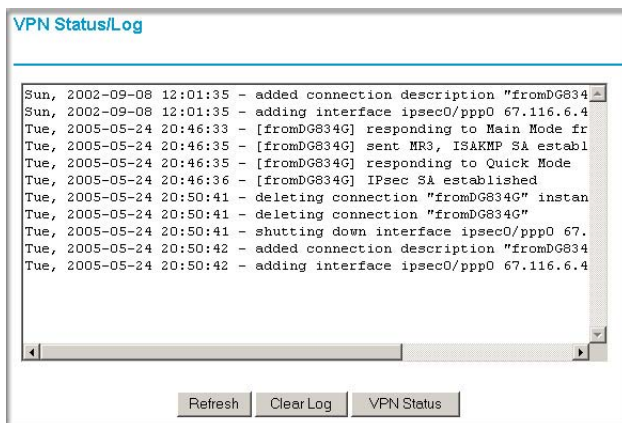

Figure B-27
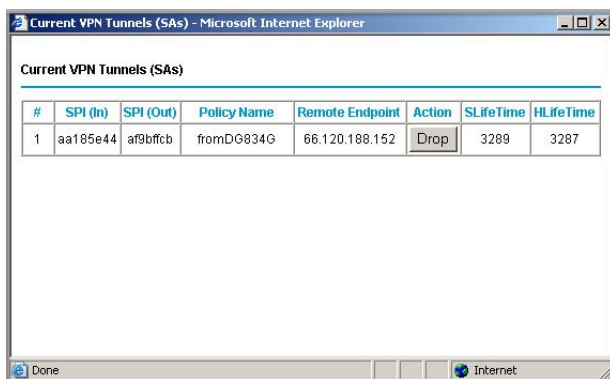
2. To view the VPN tunnels status, click VPN Status.

Figure B-28

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