Reference Manual for the ADSL Firewall Router DG834

NETGEAR

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

202-10005-05
June 2005

Trademarks

NETGEAR is a trademark of Netgear, Inc.

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

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

Statement of Conditions

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

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

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

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

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

Federal Communications Commission (FCC) Radiation Exposure Statement

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

EN 55 022 Declaration of Conformance

This is to certify that the DG834 ADSL Firewall Router is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

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

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

Certificate of the Manufacturer/Importer

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

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your DG834 ADSL Firewall Router.

World Wide Web

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

Product and Publication Details

Model Number:	DG834
Publication Date:	June 2005
Product Family:	router
Product Name:	DG834 ADSL Firewall Router
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10005-05

Contents

Appendix D
Virtual Private Networking

Appendix E
NETGEAR VPN Configuration

Chapter 1
About This Manual

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

Audience, Scope, Conventions, and Formats

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

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

italics	Emphasis, books, CDs, URL names
bold	User input
`fixed`	Screen text, file and server names, extensions, commands, IP addresses

This guide uses the following formats to highlight special messages:

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

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

Table 1-2. Manual Scope

Product Version	DG834 ADSL Firewall Router
Manual Publication Date	June 2005

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/DG834.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A TOC button that displays the table of contents and an Index 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 Knowledge Base button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

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

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

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

- **Printing a Chapter**.

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

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

    Note: Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

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

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

- **Printing the Full Manual**.

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

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

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

Chapter 2
Introduction

This chapter describes the features of the NETGEAR DG834 ADSL Firewall Router. The DG834 ADSL router is a combination of a built-in ADSL modem, router, 4-port switch, and firewall which enables your entire network to safely share an Internet connection that otherwise is used by a single computer.

Note: If you are unfamiliar with networking and routing, refer to Appendix B, "Network and Routing Basics" to become more familiar with the terms and procedures used in this manual.

About the Router

The DG834 ADSL Firewall Router provides continuous, high-speed 10/100 Ethernet access between your Ethernet devices. The DG834 ADSL router enables your entire network to share an Internet connection through the built-in ADSL modem that otherwise is used by a single computer. With minimum setup, you can install and use the router within minutes.

The DG834 ADSL router provides multiple Web content filtering options, plus e-mail browsing activity, reporting, and instant alerts. Parents and network administrators can establish restricted access policies based on time of day, Web site addresses, and address keywords. They can also share high-speed ADSL Internet access for up to 253 personal computers. The included firewall and Network Address Translation (NAT) features protect you from hackers.

Key Features

The DG834 ADSL router provides the following features:

- A built-in ADSL modem
- A powerful, true firewall
- Easy, Web-based setup for installation and management

- Extensive Internet protocol support
- Trustworthy VPN Communications over the Internet
- VPN Wizard for easy VPN configuration
- Content filtering
- Auto Sensing and Auto Uplink™ LAN Ethernet connections

These features are discussed below.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the DG834 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection
  Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents
  The DG834 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to email the log to you at specified intervals. You can also configure the router to send immediate alert messages to your email address or email pager whenever a significant event occurs.

Easy Installation and Management

You can install, configure, and operate the DG834 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-based management
  Browser-based configuration allows you to easily configure your router from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- Smart Wizard
  The router automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.

- Remote management
  The router allows you to log in to the Web management interface from a remote location via the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.
- Diagnostic functions
  The router incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the router. You can use these diagnostic functions directly from the DG834 when you are connected on the LAN or when you are connected over the Internet via the remote management function.
- Visual monitoring
  The router's front panel LEDs provide an easy way to monitor its status and activity.
- Flash erasable programmable read-only memory (EPROM) for firmware upgrades.

Protocol Support

The DG834 supports Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). Appendix B, "Network and Routing Basics" provides further information on TCP/IP.

- The Ability to Enable or Disable IP Address Sharing by NAT
  The DG834 allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account. This feature can also be turned off completely while using the DG834 if you want to manage the IP address scheme yourself.
- Automatic Configuration of Attached PCs by DHCP
  The DG834 dynamically assigns network configuration information, including IP, router, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- DNS Proxy
  When DHCP is enabled and no DNS addresses are specified, the router provides its own address as a DNS server to the attached PCs. The router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- Classical IP (RFC 1577)
  Some Internet service providers, in Europe for example, use Classical IP in their ADSL services. In such cases, the router is able to use the Classical IP address from the ISP.

- PPP over Ethernet (PPPoE)
  PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an ADSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your computer.
- PPP over ATM (PPPoA)
  PPP over ATM is a protocol for connecting remote hosts to the Internet over an ADSL connection by simulating an ATM connection.
- Dynamic DNS
  Dynamic DNS services allow remote users to find your network using a domain name when your IP address is not permanently assigned. The router contains a client that can connect to many popular Dynamic DNS services to register your dynamic IP address.
- Universal Plug and Play (UPnP)
  UPnP is a networking architecture that provides compatibility between networking technologies. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

Virtual Private Networking (VPN)

The DG834 ADSL router provides a secure encrypted connection between your local area network (LAN) and remote networks or clients. It includes the following VPN features:

- Supports 8 VPN connections.
- Supports industry standard VPN protocols
  The DG834 ADSL router supports standard Manual or IKE keying methods, standard MD5 and SHA-1 authentication methods, and standard DES and 3DES encryption methods. It is compatible with many other VPN products.
- Supports 3DES encryption for maximum security.
- VPN Wizard based on VPNC recommended settings.

Content Filtering

With its content filtering feature, the DG834 prevents objectionable content from reaching your PCs. The router allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the router to log and report attempts to access objectionable Internet sites.

Auto Sensing and Auto Uplink™ LAN Ethernet Connections

With its internal 4-port 10/100 switch, the DG834 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The local LAN ports are autosensing and capable of full-duplex or half-duplex operation.

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

What’s in the Box?

The product package should contain the following items:

- DG834 ADSL Firewall Router
- AC power adapter (varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable
- Microfilters (quantity and type vary by region)
- *ADSL Firewall Router Resource CD*, including:
  - This guide
  - Application Notes
- A Printed Quick Installation Guide
- Warranty and Support Information Cards

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

The Router’s Front Panel

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

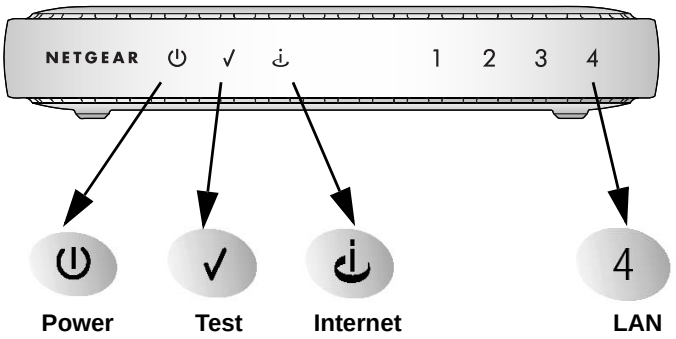


Figure 2-1: DG834 Front Panel

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

Table 2-1. LED Descriptions

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

The Router's Rear Panel

The rear panel of the DG834 ADSL Firewall Router (Figure 2-2) contains port connections.

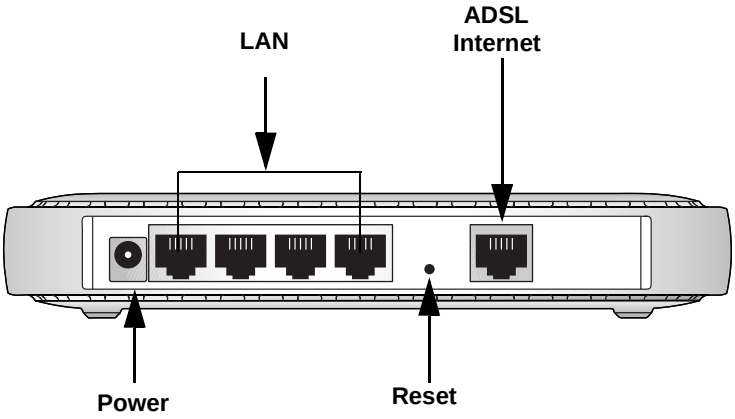


Figure 2-2: DG834 Rear Panel

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

- AC power adapter outlet
- Four Local Ethernet RJ-45 ports for connecting the router to the local computers
- Factory Default Reset push button
- ADSL port for connecting the router to an ADSL line

Chapter 3
Connecting the Router to the Internet

This chapter describes how to set up the router on your Local Area Network (LAN) and connect to the Internet. It describes how to configure your DG834 ADSL Firewall Router for Internet access using the Setup Wizard, or how to manually configure your Internet connection.

What You Need Before You Begin

You need to prepare the following before you can establish an Internet connection through your router:

1. The router connected to an ADSL line and a computer properly connected to the router as explained below.
2. Active Internet service such as that provided by an ADSL account.
3. The Internet Service Provider (ISP) configuration information for your DSL account.

Note: If you purchased the DG834 in a country where a microfilter is not included, you must acquire one.

ADSL Microfilter Requirements

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

ADSL Microfilter

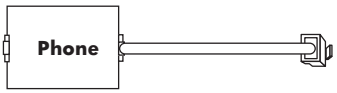


Figure 3-1: ADSL microfilter

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

Note: Do not connect the DG834 to the ADSL line through a microfilter unless the microfilter is a combination microfilter/splitter specifically designed for this purpose. Doing so will prevent the built-in ADSL modem in the DG834 from establishing a connection to the Internet. If you have any doubts about this, connect the DG834 directly to the ADSL line.

ADSL Microfilter with Built-In Splitter

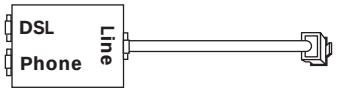


Figure 3-2: ADSL microfilter with built-in splitter

Use an ADSL microfilter with built-in splitter when there is a single wall outlet which must provide connectivity for both the DG834 and telephone equipment.

Ethernet Cabling Requirements

The DG834 ADSL router connects to your Ethernet LAN via twisted-pair cables. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your router.

Computer Hardware Requirements

To use the DG834 ADSL router on your network, each computer must have an installed Ethernet adapter and an Ethernet cable, or a 802.11g wireless adapter.

LAN Configuration Requirements

For the initial connection to the Internet and configuration of your router, you need to connect a computer to the router which is set to automatically get its TCP/IP configuration from the router via DHCP.

Note: Please refer to Appendix C, “Preparing Your Network” for assistance with DHCP configuration.

Internet Configuration Requirements

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

- Virtual Path Identifier (VPI)/Virtual Channel Indentifier (VCI) parameters
- Multiplexing Method
- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses
- Fixed or Static IP Address

Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information.

- 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 or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
    - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties.
    - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties.
    - For Macintosh computers, open the TCP/IP or Network control panel.
- You can also refer to the *DG834 Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the next page.

Record Your Internet Connection Information

Print the following page. Fill in the configuration parameters from your Internet Service Provider (ISP).

ISP Multiplexing Method and Virtual Circuit Number: The default settings of your DG834 ADSL Firewall Router will work fine for most ISPs. However, some ISPs use a specific Multiplexing Method or a Virtual Circuit Number for either the Virtual Path Identifier (VPI) or Virtual Channel Identifier (VCI). If your ISP provided you with a specific Multiplexing Method or VPI/VCI number, then fill in the following:

Multiplexing Method, circle one: LLC-based or VC-based
VPI: _____ A number between 0 and 255.
VCI: _____ A number between 1 and 65535.

ISP Login Name: The login name and password are case sensitive and must be entered exactly as given by your ISP. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you use a login name and password, then fill in the following:

Login Name: _____ Password: _____

Service Name: _____

Fixed or Static IP Address: If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: _____._____._____._____
Router IP Address: _____._____._____._____
Subnet Mask: _____._____._____._____

ISP DNS Server Addresses: If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: _____._____._____._____

Secondary DNS Server IP Address: _____._____._____._____

Host and Domain Names: Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you did not get host or domain names, use the following examples as a guide:

- If your main e-mail account with your ISP is **aaa@yyy.com**, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _____ ISP Domain Name: _____

Connecting the DG834 to Your LAN

This section provides instructions for connecting the DG834 ADSL router.

Note: The Resource CD included with your router contains an animated Installation Assistant to help you through this procedure.

How to Connect the Router

There are four steps to connecting your firewall:

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

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

1. Install ADSL Filters on the Phone Lines.

a. You need to install a filter on every telephone or device that shares the same phone number as your ADSL router. Select the filter that came with your router.

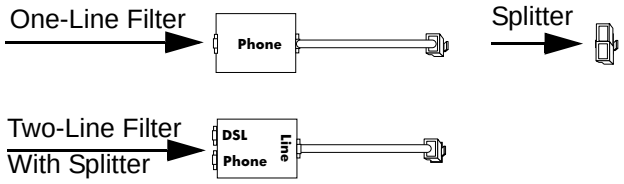


Figure 3-3: ADSL microfilters

Note: If you purchased the DG834 in a country where the filter is not included, you must acquire one.

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

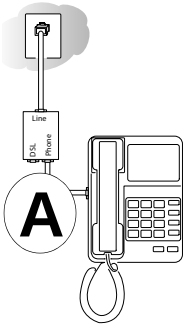


Figure 3-4: Connecting an ADSL microfilter and phone

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

2. CONNECT THE DG834 TO THE ADSL FILTERS.

Note: Improperly connecting a filter to your DG834 ADSL router will block your ADSL connection.

a. Turn off your computer.

b. Connect the ADSL port of the DG834 to the ADSL port (**B)** of the two-line filter:

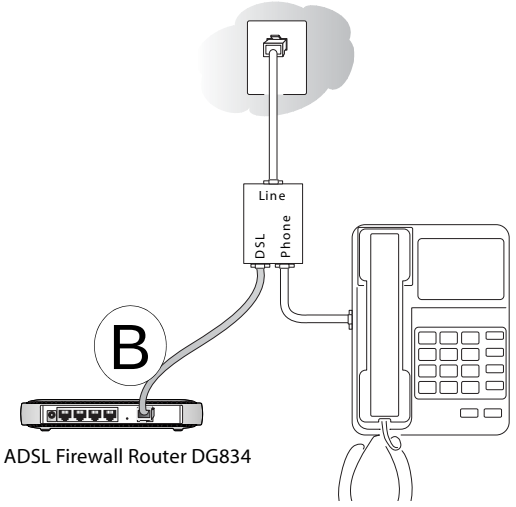


Figure 3-5: Connecting the DG834 ADSL router to an ADSL microfilter and phone

c. Connect the Ethernet cable (**C)** from your DG834's LAN port to the Ethernet adapter in your computer.

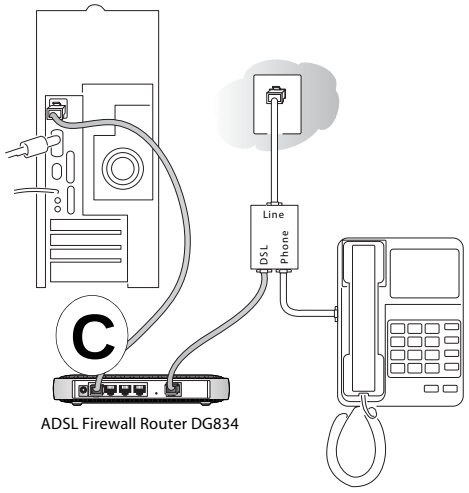


Figure 3-6: Connecting a computer to the DG834 ADSL router

Note: The DG834 ADSL router incorporates Auto Uplink™ technology. Each Ethernet LAN port will automatically sense whether the cable plugged into the port should have a 'normal' connection (for example, connecting to a computer) or an 'uplink' connection (for example, connecting to a switch or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

d. Connect the power adapter to the router and plug it in to a power outlet. Verify the following:

The power light is lit after turning on the router.

The ADSL link light is solid green, indicating a link has been established to the ADSL network.

e. Now, turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically. Verify the following:

The local lights are lit for any connected computers.

3. **LOG IN TO THE DG834.**

Note: Your computer needs to be configured for DHCP. For instructions on configuring for DHCP, please see Appendix C, "Preparing Your Network".

a. Connect to the router by typing *http://192.168.0.1* in the address field of Internet Explorer or Netscape® Navigator.

Figure 3-7: Connect to the router

A login window opens as shown below:

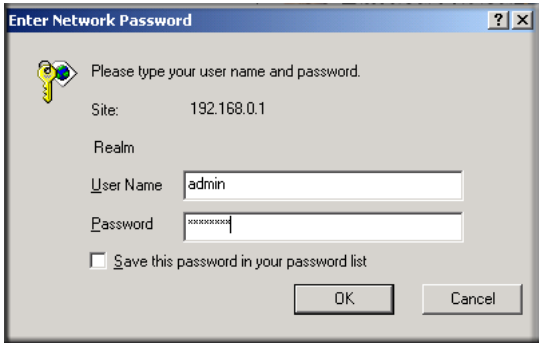


Figure 3-8: Login window

b. When prompted, enter **admin** for the user name and **password** for the password, both in lower case letters. After logging in, you will see the menu below.

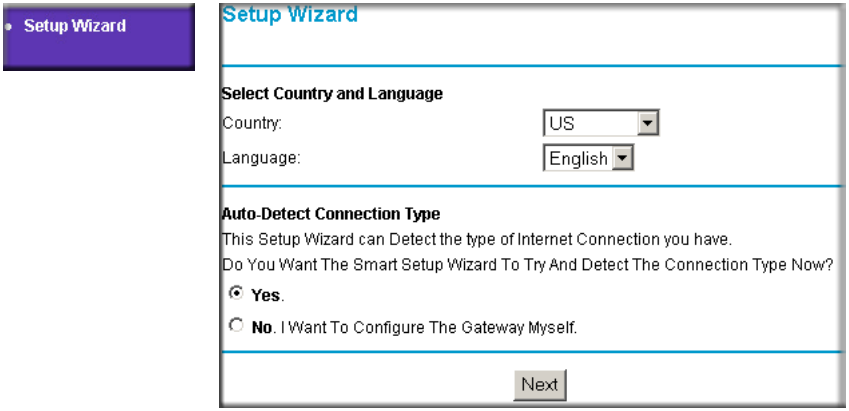


Figure 3-9: Setup Wizard

4. **CONNECT TO THE INTERNET**

   The router is now properly attached to your network. You are now ready to configure your router to connect to the Internet. There are two ways you can configure your router to connect to the Internet:

   a. Let the DG834 auto-detect the type of Internet connection you have and configure it. See "Auto-Detecting Your Internet Connection Type" on page 3-9 for instructions.

   b. Manually choose which type of Internet connection you have and configure it. See "Manually Configuring Your Internet Connection" on page 3-14 for instructions.

These options are described below. In either case, unless your ISP automatically assigns your configuration automatically via DHCP, you need the configuration parameters from your ISP you recorded in "Record Your Internet Connection Information" on page 3-3.

Auto-Detecting Your Internet Connection Type

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

1. If your router has not yet been configured, the Setup Wizard shown in Figure 3-9 should launch automatically.

Note: If instead of the Setup Wizard menu, the main menu of the router's Configuration Manager as shown in Figure 3-15 appears, click the Setup Wizard link in the upper left to bring up this menu.

2. You must select a country and language. Language choices are English, French, German, and Italian. After you change the language, the remaining setup screens change to the language of your choice.
3. Select Yes to allow the router to automatically determine your connection.
4. Click Next.

   The Setup Wizard will now check for the following connection types:

   - Dynamic IP assignment
   - A login protocol such as PPPoE or PPPoA
   - Classical IP over ATM (RFC1577)
   - Fixed IP address assignment

   Next, the Setup Wizard will report which connection type it has discovered, and then display the appropriate configuration page. If the Setup Wizard finds no connection, you will be prompted to check the physical connection between your router and the ADSL line. When the connection is properly made, the router's Internet LED should be on.
5. The ADSL settings for the multiplexing method and VPI/VCI will update with the preset defaults. The multiplexing method preset default settings will usually work. Only change the multiplexing method if you are sure your ISP requires Virtual Path Identifier (VPI) or Virtual Channel Identifier (VCI) settings that are different from the default values.

   Incorrect VPI or VCI settings will prevent you from connecting to the Internet. To change these settings, click the ADSL Settings link on the main menu. See "ADSL Settings" on page 3-19 for more details.

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

Wizard-Detected PPPoE Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over Ethernet (PPPoE), you will be directed to the PPPoE page shown in Figure 3-10:

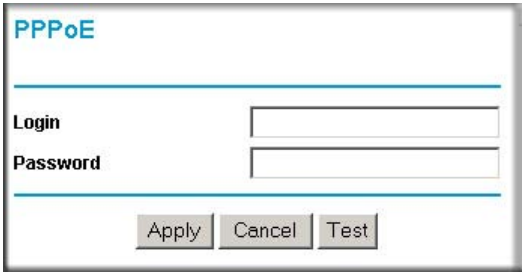


Figure 3-10: Setup Wizard menu for PPPoE login accounts

Enter the PPPoE login user name and password.

Wizard-Detected PPPoA Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over ATM (PPPoA), you will be directed to the PPPoA page shown in Figure 3-11 below:

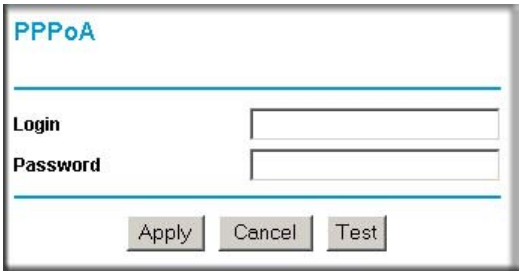


Figure 3-11: Setup Wizard menu for PPPoA login accounts

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

Wizard-Detected Dynamic IP Account Setup

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the page shown in Figure 3-12 below:

Figure 3-12: Setup Wizard menu for Dynamic IP address

Click Apply to set Dynamic IP as the connection method.

Wizard-Detected IP Over ATM Account Setup

If the Setup Wizard determines that your Internet service account uses IP over ATM Classical IP assignment (RFC1577), you will be directed to the page shown in Figure 3-13 below:

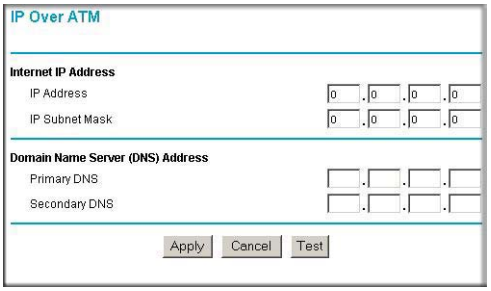


Figure 3-13: Setup Wizard menu for IP over ATM (Classical IP) address

1. Enter your assigned IP Address and Subnet Mask. This information should have been provided to you by your ISP. You need the configuration parameters from your ISP you recorded in "Record Your Internet Connection Information" on page 3-3.
2. Enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

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

4. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 8, “Troubleshooting”.

Wizard-Detected Fixed IP (Static) Account Setup

If the router determines that your Internet service account uses Fixed IP assignment, you will be directed to the page shown in Figure 3-14 below:

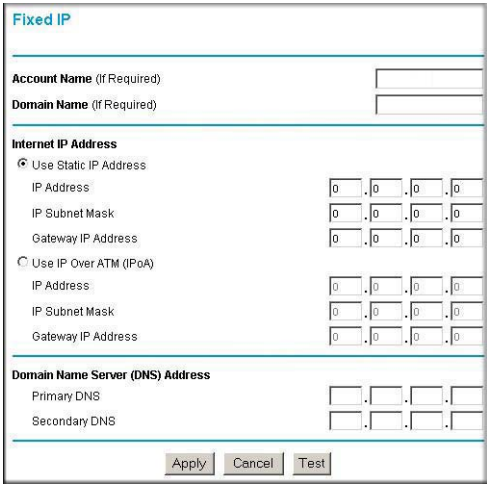


Figure 3-14: Setup Wizard menu for Fixed IP address

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

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

5. Click Apply to save the settings.
6. Click the Test button to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 8, "Troubleshooting".

Testing Your Internet Connection

After completing the Internet connection configuration, your can test your Internet connection. Log in to the router, then, from the Basic Settings link in the Setup menu, click the Test button. If the NETGEAR Web site does not appear within one minute, refer to Chapter 8, "Troubleshooting".

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

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

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

Manually Configuring Your Internet Connection

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

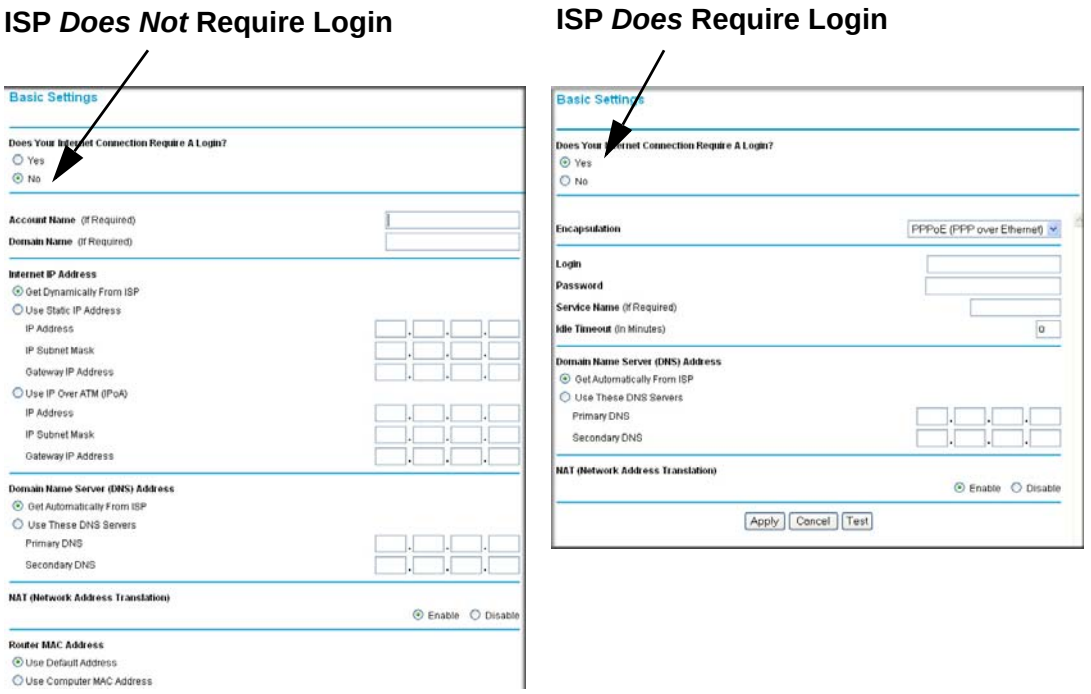


Figure 3-15: Basic Settings menu

How to Perform Manual Configuration

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

1. Select your country and language. Language choices are English, French, German, and Italian. After you change the language, the remaining setup screens change to the language of your choice.
2. Select No to manually configure your router connection.
3. Click Next.
4. Manually configure the router in the Basic Settings menu shown in Figure 3-15.
5. Follow the instructions below according to the encapsulation method and whether your Internet connection requires a login. The following methods are available:
   - Internet Connection Requires Login and Uses PPPoE
   - Internet Connection Requires Login and Uses PPPoA

- Internet Connection Does Not Require a Login

6. Usually the default ADSL Settings work fine for most ISPs and you can skip this step. If you have any problems with your connection, check the ADSL Settings. See "ADSL Settings" on page 3-19 for more details.

Internet Connection Requires Login and Uses PPPoE

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

   Note: You will no longer need to launch the ISP's login program on your computer in order to access the Internet. When you start an Internet application, your router automatically logs you in.

2. Choose PPPoE for the encapsulation method.
3. Enter the login name (frequently the email address your ISP provided), password, and service name (if required).
4. If you want to change the login timeout, enter a new value in minutes. This determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of zero means never log out.
5. When a connection uses PPPoE, the IP address is normally assigned automatically. However, the DG834 allows this address to be set manually.

   - Select "Get Automatically from ISP" if your ISP assigns your IP address.
   - Select "Use Static IP Address" if your ISP gives you a statically assigned address.

6. The DNS server is used to look up site addresses based on their names.

   - Select "Get Automatically from ISP" if your ISP uses DHCP to assign your DNS servers. Your ISP will automatically assign this address.
   - Select "Use These DNS Servers" if your ISP gave you one or two DNS addresses. Type the primary and secondary addresses.

7. You should only disable NAT if you are sure you do not require it. NAT automatically assigns private IP addresses (192.168.0.x) to LAN connected devices. When NAT is disabled, only standard routing is performed by this router.
   Classical routing lets you directly manage the IP addresses the DG834 uses. Classical routing should be selected only by experienced users.

Note: Disabling NAT will reboot the router and reset all the DG834 configuration settings to the factory default. Disable NAT only if you plan to install the DG834 in a setting where you will be manually administering the IP address space on the LAN side of the router.

Internet Connection Requires Login and Uses PPPoA

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

   Note: You will no longer need to launch the ISP's login program on your computer in order to access the Internet. When you start an Internet application, your router automatically logs you in.

2. Choose PPPoA for the encapsulation method.
3. Enter the login name (frequently the email address your ISP provided), and password.
4. If you want to change the login timeout, enter a new value in minutes. This determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of zero means never log out.
5. When a connection uses PPPoA, the IP address is normally assigned automatically. However, the DG834 allows this address to be set manually.
   - Select "Get Automatically from ISP" if your ISP assigns your IP address.
   - Select "Use Static IP Address" if your ISP gives you a statically assigned address.
6. The DNS server is used to look up site addresses based on their names.
   - Select "Get Automatically from ISP" if your ISP uses DHCP to assign your DNS servers. Your ISP will automatically assign this address.
7. Select "Use These DNS Servers" if your ISP gave you one or two DNS addresses. Type the primary and secondary addresses.You should only disable NAT if you are sure you do not require it. NAT automatically assigns private IP addresses (192.168.0.x) to LAN connected devices. When NAT is disabled, only standard routing is performed by this router. Classical routing lets you directly manage the IP addresses the DG834 uses. Classical routing should be selected only by experienced users.

   Note: Disabling NAT will reboot the router and reset all the DG834 configuration settings to the factory default. Disable NAT only if you plan to install the DG834 in a setting where you will be manually administering the IP address space on the LAN side of the router.

Internet Connection Does Note Require A Login

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

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

   Classical routing lets you directly manage the IP addresses the DG834 uses. Classical routing should be selected only by experienced users.

   Note: Disabling NAT will reboot the router and reset all the DG834 configuration settings to the factory default. Disable NAT only if you plan to install the DG834 in a setting where you will be manually administering the IP address space on the LAN side of the router

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

   To change the MAC address, select "Use this Computer's MAC address". The router will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. Alternatively, select "Use this MAC address" and enter it.
7. Click Apply to save your settings.
8. Click the Test button to test your Internet connection.
   If the NETGEAR Web site does not appear within one minute, refer to Chapter 8, "Troubleshooting".

ADSL Settings

The default settings of your DG834 ADSL Firewall Router will work fine for most ISPs. However, some ISPs use a specific Multiplexing Method and Virtual Circuit Number for the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI).

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

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

1. Select the ADSL Settings link from the main menu.
2. For the Multiplexing Method, select LLC-based or VC-based.
3. Type a number between 0 and 255 for the VPI. The default is 8.
4. Type a number between 1 and 65535 for the VCI. The default is 35.
5. Click Apply.

Chapter 4
Protecting Your Network

This chapter describes how to use the basic firewall features of the DG834 ADSL Firewall Router to protect your network.

Protecting Access to Your DG834 ADSL Firewall Router

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

Note: The user name and password are not the same as any user name or password your may use to log in to your Internet connection.

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

How to Change the Built-In Password

1. Log in to the 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 router.

Figure 4-1: Log in to the router

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

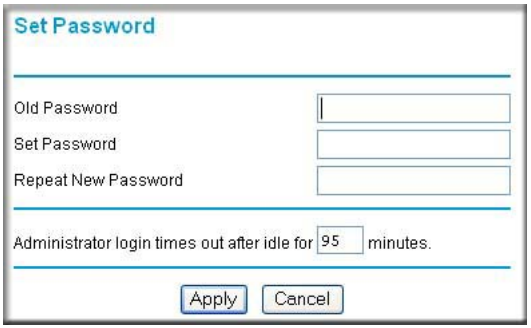


Figure 4-2: Set Password menu

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

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

Changing the Administrator Login Timeout

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

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

Configuring Basic Firewall Services

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

Blocking Keywords, Sites, and Services

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

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

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

How to Block Keywords and Sites

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

1. Log in to the 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 router.
2. Select the Block Sites link of the Security menu.

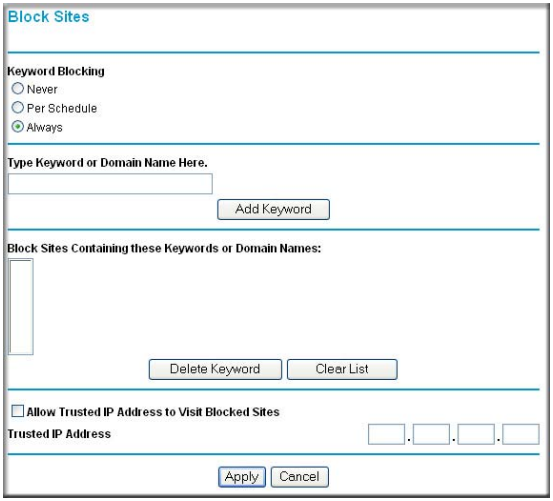


Figure 4-3: Block Sites menu

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

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

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

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

7. Click Apply to save your settings.

Firewall Rules

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

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the DG834 are:

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

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

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

To access the rules configuration of the DG834, click the Firewall Rules link on the main menu, then click Add for either an Outbound or Inbound Service.

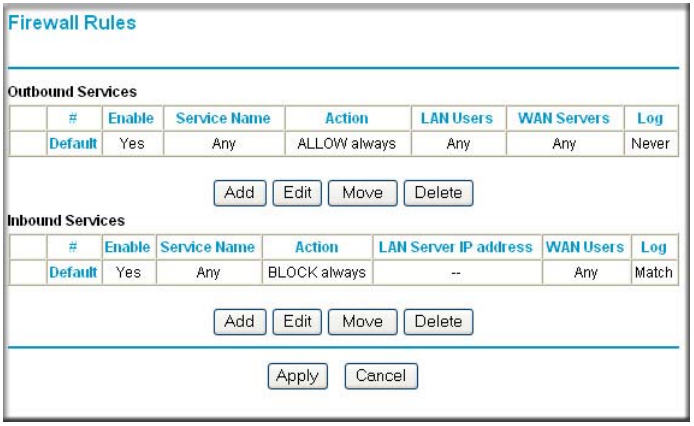


Figure 4-4: Rules menu

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

Inbound Rules (Port Forwarding)

Because the DG834 uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

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

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

Inbound Rule Example: A Local Public Web Server

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

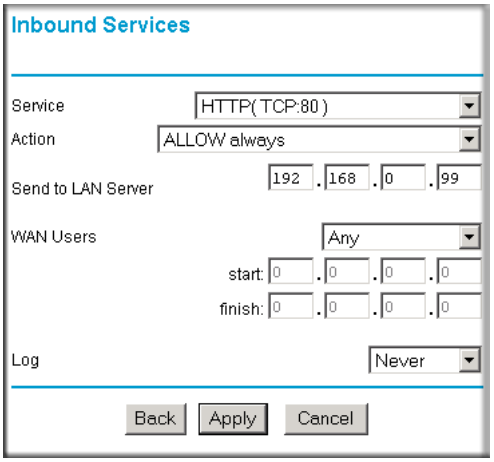


Figure 4-5: Rule example: A Local Public Web Server

The parameters are:

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

  – Any — all IP addresses are covered by this rule.
  – Address range — if this option is selected, you must enter the Start and Finish fields.
  – Single address — enter the required address in the Start field.

- Log
  You can select whether the traffic will be logged. The choices are:
  - Never — no log entries will be made for this service.
  - Always — any traffic for this service type will be logged.
  - Match — traffic of this type which matches the parameters and action will be logged.
  - Not match — traffic of this type which does not match the parameters and action will be logged.

Inbound Rule Example: Allowing Videoconferencing

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

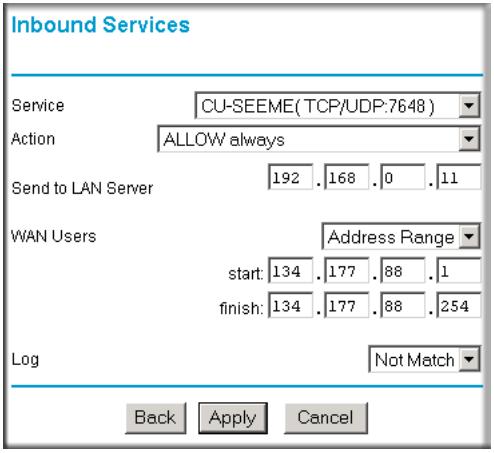


Figure 4-6: Rule example: Videoconference from Restricted Addresses

Considerations for Inbound Rules

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

- If the IP address of the local server computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer's IP address constant.
- Local computers must access the local server using the computer's local LAN address (192.168.0.11 in the example in Figure 4-6 above). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The DG834 allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on:

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

Following is an application example of outbound rules:

Outbound Rule Example: Blocking Instant Messenger

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

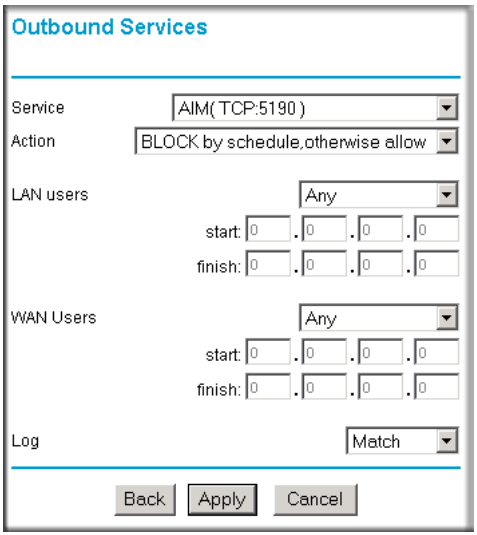


Figure 4-7: Rule example: Blocking Instant Messenger

The parameters are:

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

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

Order of Precedence for Rules

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

Outbound Services

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

Add Edit Move Delete

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
◉	1	☑	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
○	2	☑	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match

Add Edit Move Delete

Figure 4-8: Rules table with examples

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

Services

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

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

Although the DG834 already holds a list of many service port numbers, you are not limited to these choices. Use the procedure below to create your own service definitions.

How to Define Services

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

Figure 4-9: Services menu

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

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

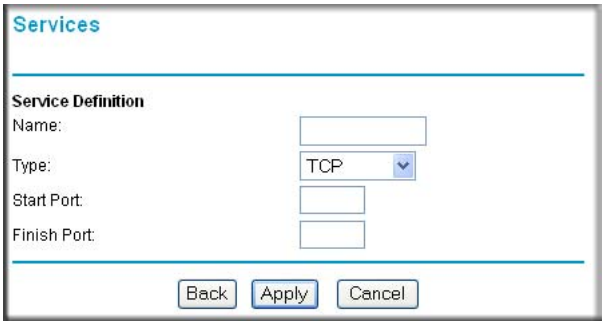


Figure 4-10: Add Services menu

4. Click Apply to save your changes.

Setting Times and Scheduling Firewall Services

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

How to Set Your Time Zone

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

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

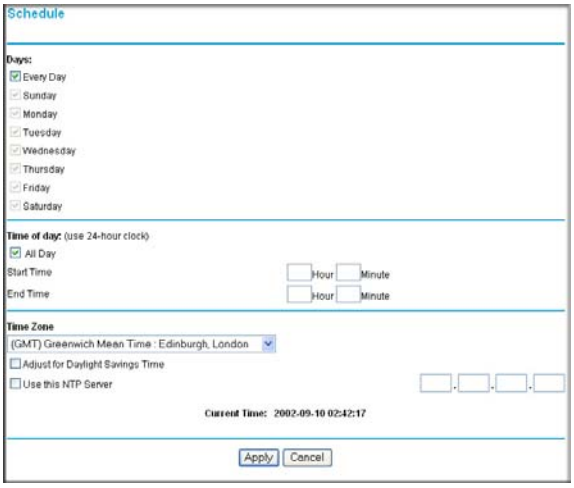


Figure 4-11: Schedule Services menu

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

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

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

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

5. Click Apply to save your settings.

How to Schedule Firewall Services

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

1. Log in to the 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 router.

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

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

Chapter 5
Managing Your Network

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

Backing Up, Restoring, or Erasing Your Settings

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

How to Back Up the Configuration to a File

1. Log in to the 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 Maintenance heading of the Main Menu, select the Backup Settings menu as seen in Figure 5-1.

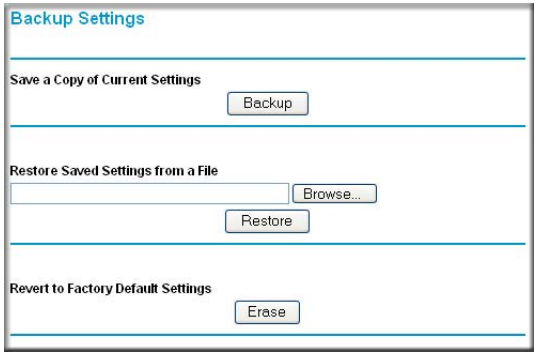


Figure 5-1: Backup Settings menu

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

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

How to Restore the Configuration from a File

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

How to Erase the Configuration

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

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

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

Note: To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See "DG834 Rear Panel" on page 2-7.

Upgrading the Router's Firmware

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

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

How to Upgrade the Router Firmware

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

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

   The Web browser used to upload new firmware into the router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or above, or Netscape Navigator 4.7 or above.

2. Log in to the 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.

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

Figure 5-2: Router Upgrade menu

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

5. Click **Upload**.

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

Network Management Information

The DG834 provides a variety of status and usage information which is discussed below.

Viewing Router Status and Usage Statistics

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

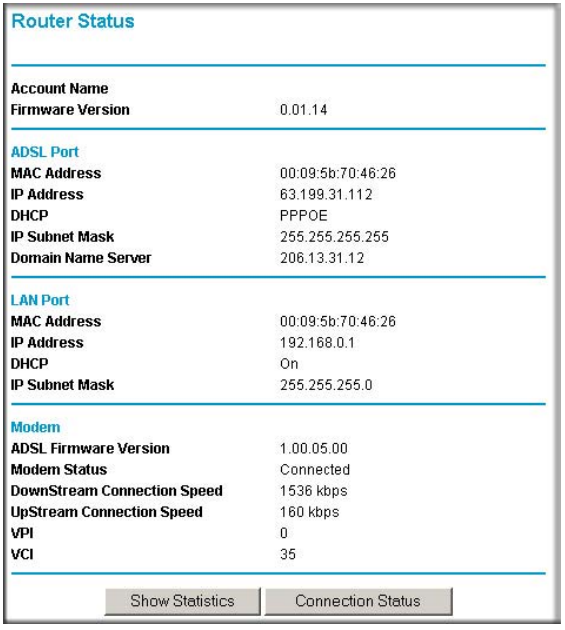


Figure 5-3: Router Status screen

The Router Status menu provides status and usage information.

This screen shows the following parameters:

Table 5-1. Menu 3.2 - Router Status Fields

Field	Description
Account Name	The Host Name assigned to the router in the Basic Settings menu.
Firmware Version	This field displays the router firmware version.
ADSL Port	These parameters apply to the Internet (ADSL) port of the router.
MAC Address	This field displays the Ethernet MAC address being used by the Internet (ADSL) port of the router.
IP Address	This field displays the IP address being used by the Internet (ADSL) port of the router. If no address is shown, the router cannot connect to the Internet.
DHCP	If None, the router will use a fixed IP address on the ADSL. If Client, the router will obtain an IP address dynamically from the ISP.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (ADSL) port of the router.
Domain Name Server (DNS)	This field displays the DNS Server IP addresses being used by the router. These addresses are usually obtained dynamically from the ISP.
LAN Port	These parameters apply to the Local (ADSL) port of the router.
MAC Address	This field displays the Ethernet MAC address being used by the Local (LAN) port of the router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.0.1.
DHCP	If OFF, the router will not assign IP addresses to PCs on the LAN. If ON, the router will assign IP addresses to PCs on the LAN.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0.
Modem	These parameters apply to the Local (WAN) port of the router.
ADSL Firmware Version	The version of the firmware.
Modem Status	The connection status of the modem.
Downstream Speed	The speed at which the modem is receiving data from the ADSL line.
Upstream Speed	The speed at which the modem is transmitting data to the ADSL line.
VPI	The Virtual Path Identifier setting.
VCI	The Virtual Channel Identifier setting.

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

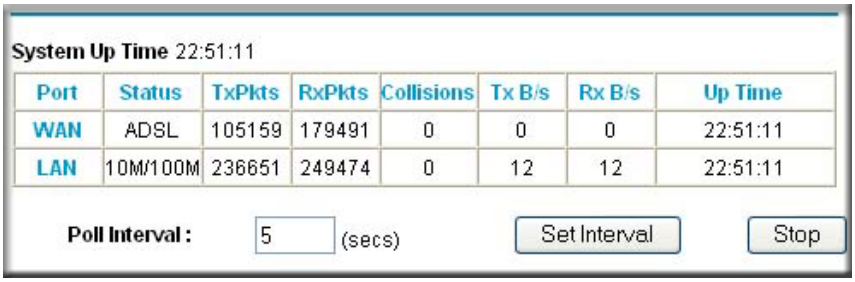


Figure 5-4: Router Statistics screen

This screen shows the following statistics:.

Table 5-1. Router Statistics Fields

Field	Description
WAN, LAN, or Serial Port	The statistics for the WAN (Internet), LAN (local), and Serial ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
Rx B/s	The average line utilization for this port.
Up Time	The time elapsed since the last power cycle or reset.
Poll Interval	Specifies the interval at which the statistics are updated in this window. Click Stop to freeze the display.

Click the Connection Status button to display router connection status, as shown in Figure 5-5 and Figure 5-6.

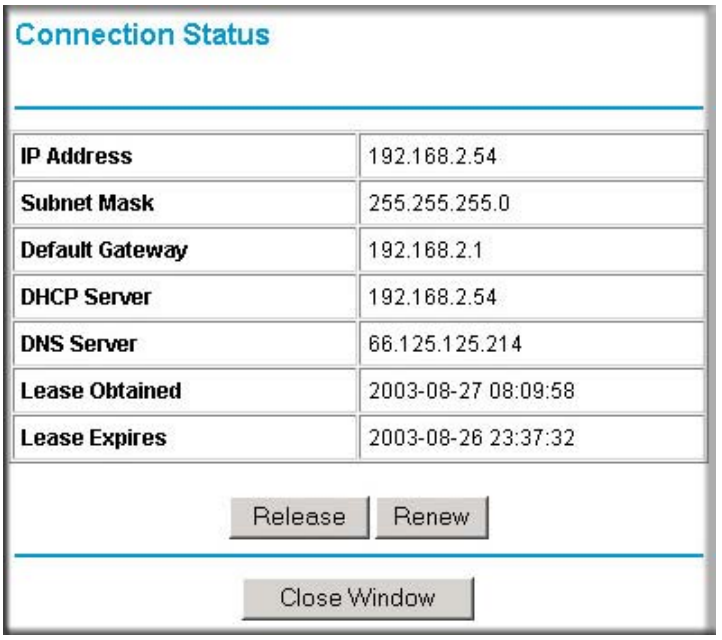


Figure 5-5: Connection Status screen for Dynamic IP

Clicking the Renew button updates the status information.

This screen shows the following statistics:

Table 5-1. Connection Status Fields for Dynamic IP

Field	Description
IP Address	The IP Address assigned to the WAN port by the ADSL Internet Service Provider.
Subnet Mask	The Network Mask assigned to the WAN port by the ADSL Internet Service Provider.
Default Gateway	The default gateway router assigned to the WAN port by the ADSL Internet Service Provider.
DHCP Server	The DHCP server's IP address.
DNS Server	The DNS server's IP address.
Lease Obtained	Date and time the lease was obtained.
Lease Expires	Date and time the lease expires.

An alternate view of the Connection Status screen is shown in Figure 5-6 below:

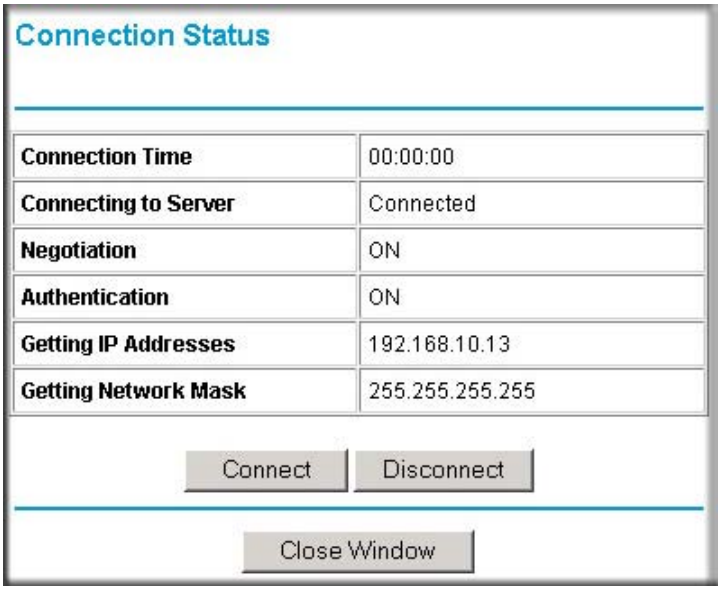


Figure 5-6: Connection Status screen for PPPoA

Clicking the Renew button updates the status information.

This screen shows the following statistics:

Table 5-1. Connection Status Fields for PPPoA

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

Viewing Attached Devices

The Attached Devices menu contains a table of all IP devices that the router has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown in Figure 5-7:

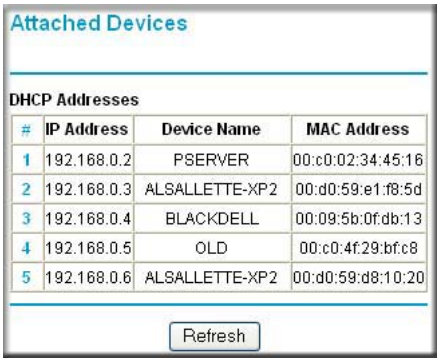


Figure 5-7: Attached Devices menu

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

Viewing, Selecting, and Saving Logged Information

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

An example of the logs file is shown below.

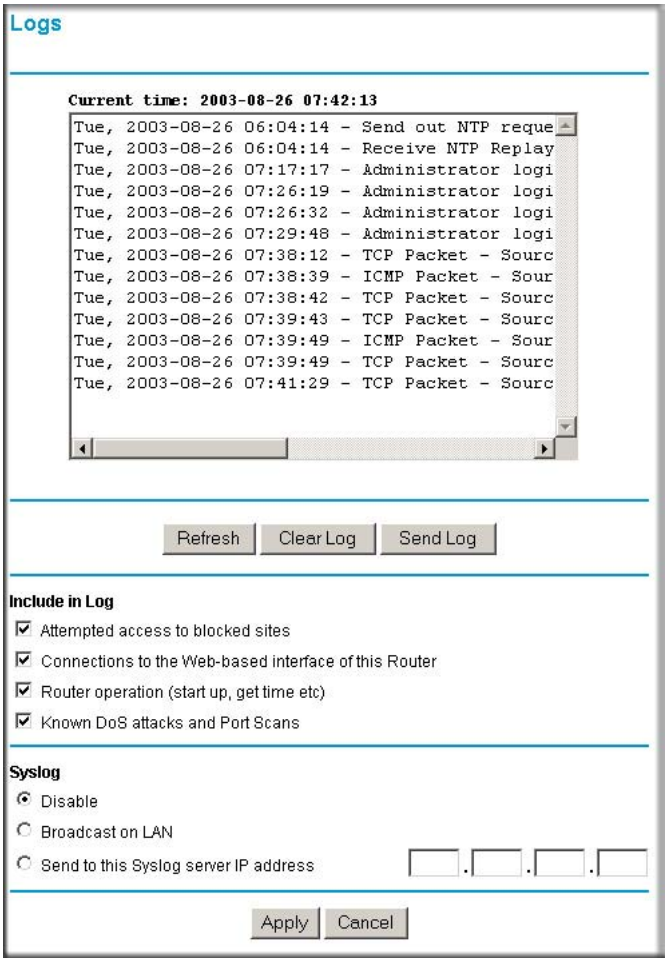


Figure 5-8: Security Logs menu

Log entries are described in Table 5-1 below:

Table 5-1. Security Log entry descriptions

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

Log action buttons are described in Table 5-2 below:

Table 5-2. Security Log action buttons

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

Selecting What Information to Log

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

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

Saving Log Files on a Server

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

Examples of Log Messages

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

Activation and Administration

```
Tue, 2002-05-21 18:48:39 - NETGEAR activated
```

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

```
Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2
Thu, 2002-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

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

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

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

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

[This entry shows when the log was emailed.]

Dropped Packets

```
Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

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

Enabling Security Event E-mail Notification

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

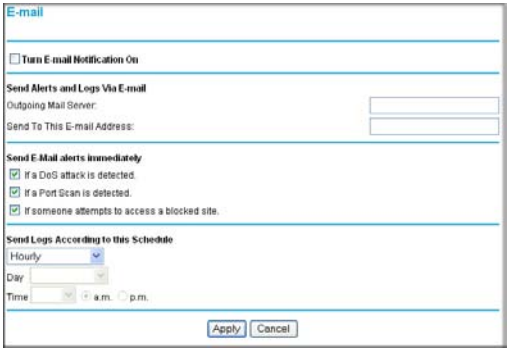


Figure 5-9: E-mail menu

- **Turn e-mail notification on**. Select this check box if you want to receive e-mail logs and alerts from the router.
- **Send alerts and logs via email**. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.
- **Send alert immediately.** Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule.** Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - Day for sending log
    Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
  - Time for sending log
    Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

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

Running Diagnostic Utilities and Rebooting the Router

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

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

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Diagnostics heading to display the menu shown in Figure 5-10.

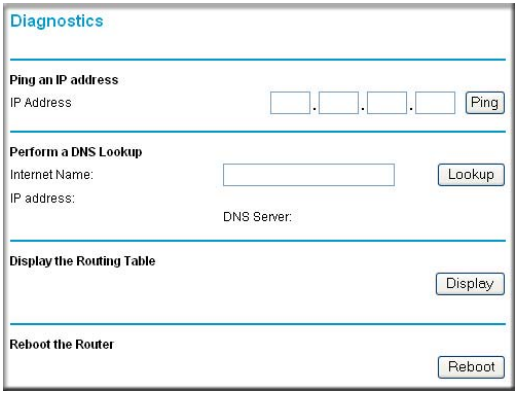


Figure 5-10: Diagnostics menu

Enabling Remote Management

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your DG834 ADSL Firewall Router.

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

Configuring Remote Management

1. Log in to the 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 Advanced section of the main menu, select the Remote Management link.
3. Select the Turn Remote Management On check box.
4. Specify what external addresses will be allowed to access the router's remote management. For security, restrict access to as few external IP addresses as practical:
   - To allow access from any IP address on the Internet, select Everyone.
   - To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.
   - To allow access from a single IP address on the Internet, select Only this Computer. Enter the IP address that will be allowed access.
5. Specify the Port Number that will be used for accessing the management interface.

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

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

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

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

Chapter 6
Advanced Configuration

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

Configuring Advanced Security

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

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

These features are discussed below.

Setting Up A Default DMZ Server

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

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

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

How to Configure a Default DMZ Server

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

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

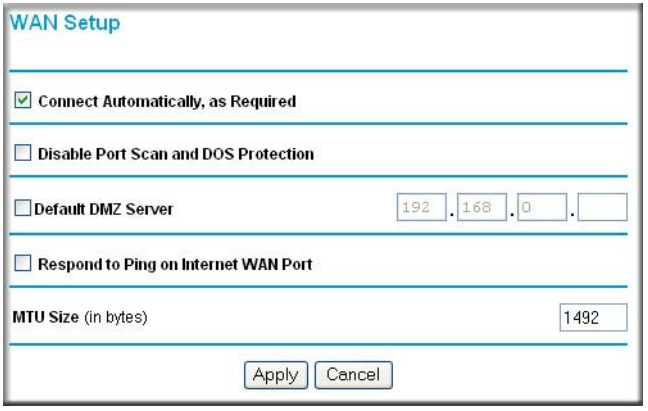


Figure 6-1: WAN Setup Page

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

Connect Automatically, as Required

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

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

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

Disable Port Scan and DOS Protection

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

Respond to Ping on Internet WAN Port

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

MTU Size

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

Configuring LAN IP Settings

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

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

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

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

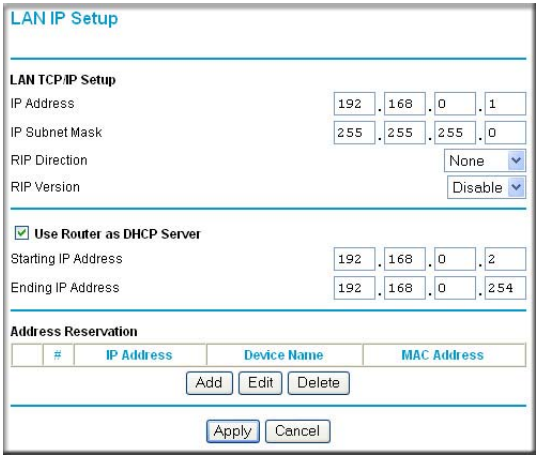


Figure 6-2: LAN IP Setup Menu

The LAN TCP/IP Setup parameters are:

- IP Address
  This is the LAN IP address of the router.
- IP Subnet Mask
  This is the LAN Subnet Mask of the 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 router.
- RIP Direction
  RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the Router sends and receives RIP packets. Both is the default.
  - — When set to Both or Out Only, the router will broadcast its routing table periodically.
  - — When set to Both or In Only, it will incorporate the RIP information that it receives.
  - — When set to None, it will not send any RIP packets and will ignore any RIP packets received.

- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the router sends. It recognizes both formats when receiving. By default, this is set for RIP-1.
  - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
  - RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
    - RIP-2B uses subnet broadcasting.
    - RIP-2M uses multicasting.

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

DHCP

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

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See “IP Configuration by DHCP”on page B-9 for an explanation of DHCP and information about how to assign IP addresses for your network.

Use Router as DHCP server

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

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

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

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

Reserved IP addresses

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

To reserve an IP address:

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

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

To edit or delete a reserved address entry:

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

How to Configure LAN TCP/IP Settings

1. Log in to the router at its default LAN address of *http://192.168.0.1* with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu, under Advanced, click the LAN IP Setup link to view the menu, shown in Figure 6-3:

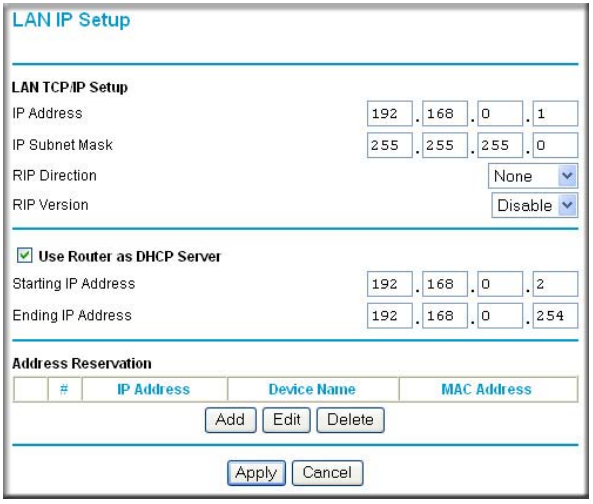


Figure 6-3: LAN IP Setup Menu

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

Configuring Dynamic DNS

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

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

How to Configure Dynamic DNS

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

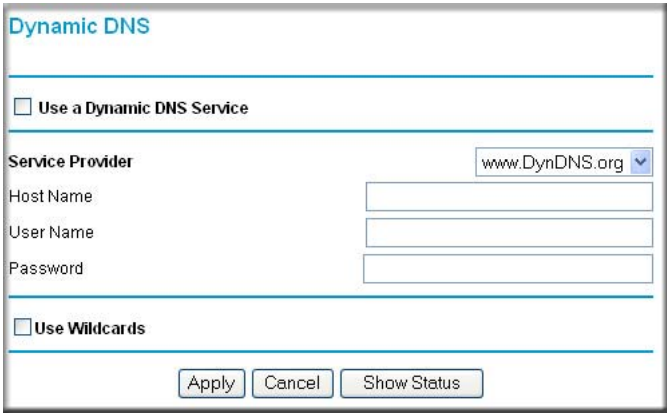


Figure 6-4: Dynamic DNS menu

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

7. Type the User Name for your dynamic DNS account.
8. Type the Password (or key) for your dynamic DNS account.
9. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the Use wildcards check box to activate this feature.
   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
10. Click Apply to save your configuration.

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

Using Static Routes

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

Static Route Example

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

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

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

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

In this example:

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

How to Configure Static Routes

1. Log in to the router at its default LAN address of *http://192.168.0.1* with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, click Static Routes to view the Static Routes menu, shown in Figure 6-5.

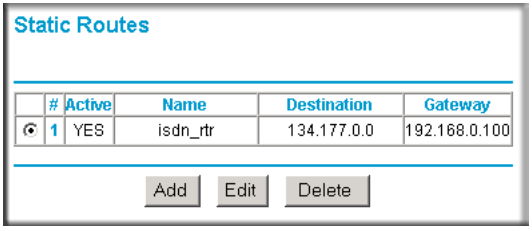


Figure 6-5: Static Routes Table

3. To add or edit a Static Route:

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

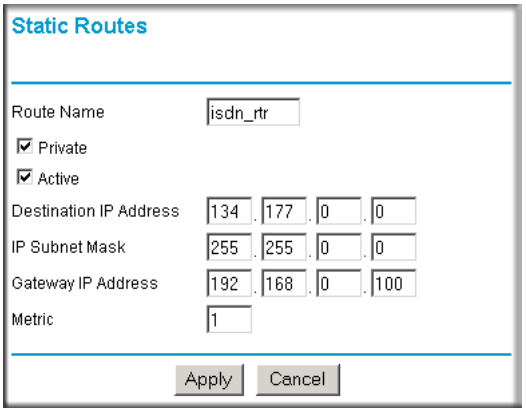


Figure 6-6: Static Route Entry and Edit Menu

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

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

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

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

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

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

   h. Type a number between 1 and 15 as the Metric value. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.

4. Click **Apply** to have the static route entered into the table.

Universal Plug and Play (UPnP)

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

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

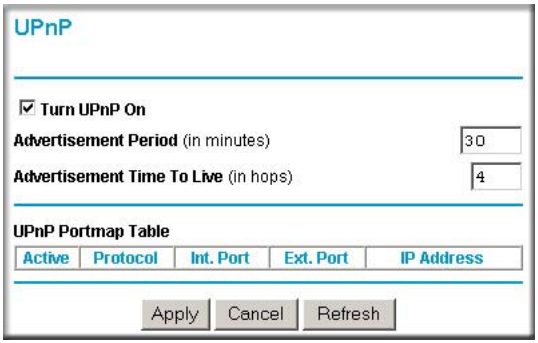


Figure 6-7: Universal Plug and Play menu

2. Fill out the UPnP screen:

   - **Turn UPnP On**: UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the Router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the Router.
   - **Advertisement Period**: The Advertisement Period is how often the Router will advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time To Live**: The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.

- **UPnP Portmap Table**: The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the Router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

3. To save, cancel or refresh the table:

   a. Click Apply to save the new settings to the Router.

   b. Click Cancel to disregard any unsaved changes.

   c. Click Refresh to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Chapter 7
Virtual Private Networking (Advanced Feature)

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

This chapter is organized as follows:

- "Overview of VPN Configuration" on page 7-2 provides an overview of the two most common VPN configurations: Client-to-Gateway and Gateway-to-Gateway.
- "Planning a VPN" on page 7-3 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 7-6 summarizes the three ways to configure a VPN tunnel: VPN Wizard (recommended for most situations), Auto Policy, and Manual Policy.
- "How to Set Up a Client-to-Gateway VPN Configuration" on page 7-6 provides the steps needed to configure a VPN tunnel between a remote PC and a network gateway using the VPN Wizard and the NETGEAR ProSafe VPN Client.
- "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-20 provides the steps needed to configure a VPN tunnel between two network gateways using the VPN Wizard.
- "VPN Tunnel Control" on page 7-27 provides the step-by-step procedures for activating, verifying, deactivating, and deleting a VPN tunnel once the VPN tunnel has been configured.
- "How to Set Up VPN Tunnels in Special Circumstances" on page 7-35 provides the steps needed to configure VPN tunnels when there are special circumstances and the VPNC recommended defaults of the VPN Wizard are inappropriate. The two alternatives for configuring VPN tunnels are Auto Policy and Manual Policy.

Overview of VPN Configuration

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

Client-to-Gateway VPN Tunnels

Client-to-Gateway VPN Tunnels provide secure access from a remote PC, such as a telecommuter connecting to an office network (see Figure 7-1).

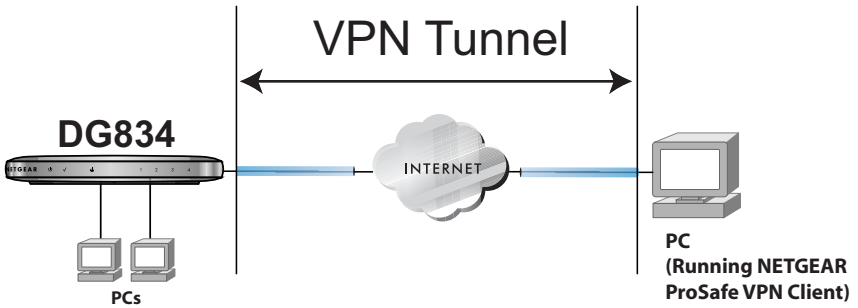


Figure 7-1: Client-to-Gateway VPN Tunnel

A VPN client access allows a remote PC to connect to your network from any location on the Internet. In this case, the remote PC is one tunnel endpoint, running the VPN client software. The DG834 ADSL router on your network is the other tunnel endpoint. See "How to Set Up a Client-to-Gateway VPN Configuration" on page 7-6 to set up this configuration.

Gateway-to-Gateway VPN Tunnels

- Gateway-to-Gateway VPN Tunnels provide secure access between networks, such as a branch or home office and a main office (see Figure 7-2).

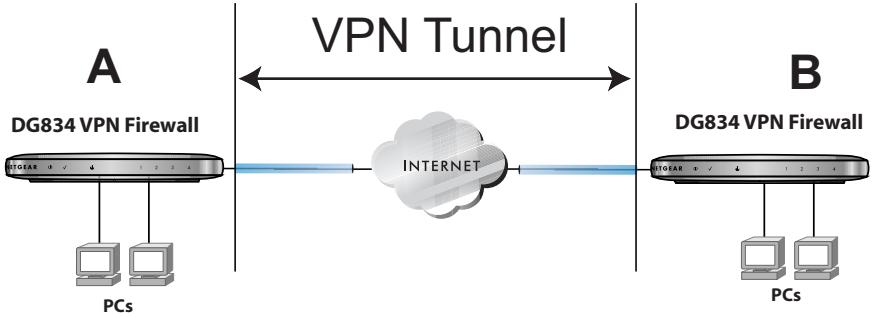


Figure 7-2: Gateway-to-Gateway VPN Tunnel

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 DG834s on each end of the tunnel to form the VPN tunnel end points. See "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-20 to set up this configuration.

Planning a VPN

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

Table 7-1. VPN Tunnel Configuration Worksheet

Connection Name:	
Pre-Shared Key:	
Secure Association -- Main Mode or Manual Keys:	
Perfect Forward Secrecy -- Enabled or Disabled:	
NETBIOS -- Enabled or Disabled:	
Encryption Protocol -- DES or 3DES:	
Authentication Protocol -- MD5 or SHA-1:	
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	
Key Life in seconds:	
IKE Life Time in seconds:	

VPN Endpoint	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)

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

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

- Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will either endpoint use Fully Qualified Domain Names (FQDNs)? FQDNs supplied by Dynamic DNS providers (see "The Use of a Fully Qualified Domain Name (FQDN)" on page E-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.

- What method will you use to configure your VPN tunnels?
  - The VPN Wizard using VPNC defaults (see Table 7-2)
  - The typical automated Internet Key Exchange (IKE) setup (see "Using Auto Policy to Configure VPN Tunnels" on page 7-36)
  - A Manual Keying setup in which you must specify each phase of the connection (see "Using Manual Policy to Configure VPN Tunnels" on page 7-48)?

Table 7-2. 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
NETBIOS	Enabled

- What level of IPSec VPN encryption will you use?
  - DES - The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
  - 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- What level of authentication will you use?
  - MDS: 128 bits, faster but less secure.
  - SHA-1: 160 bits, slower but more secure.

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

VPN Tunnel Configuration

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

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
  - See "How to Set Up a Client-to-Gateway VPN Configuration" on page 7-6.
  - See "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-20.
- See "Using Auto Policy to Configure VPN Tunnels" on page 7-36 when the VPN Wizard and its VPNC defaults (see Table 7-2 on page 7-5) 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 7-48 when the VPN Wizard and its VPNC defaults (see Table 7-2 on page 7-5) are not appropriate for your special circumstances and you must specify each phase of the connection. You manually enter all the authentication and key parameters. You have more control over the process, however the process is more complex and there are more opportunities for errors or configuration mismatches between your DG834 and the corresponding VPN endpoint gateway or client workstation.

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

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway (see Figure 7-3) involves the following two steps:

- "Step 1: Configuring the Client-to-Gateway VPN Tunnel on the DG834" on page 7-7 uses the VPN Wizard to configure the VPN tunnel between the remote PC and network gateway.
- "Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC" on page 7-12 configures the NETGEAR ProSafe VPN Client endpoint.

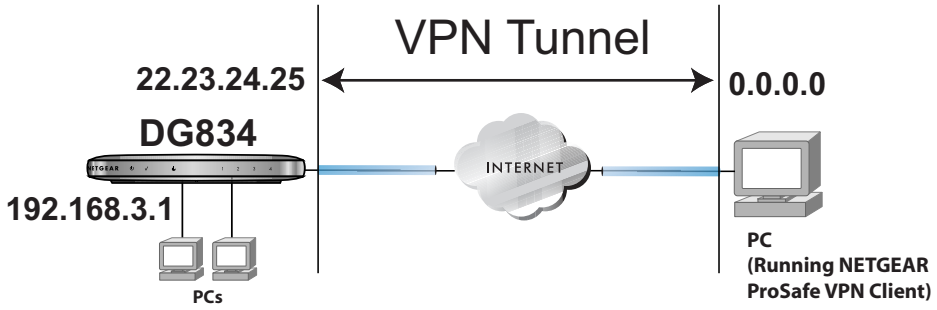


Figure 7-3: Client-to-Gateway VPN Tunnel

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

Note: This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in Table 7-2 on page 7-5. If you have special requirements not covered by these VPNC-recommended parameters, refer to "How to Set Up VPN Tunnels in Special Circumstances" on page 7-35 to set up the VPN tunnel.

The worksheet below identifies the parameters used in the following procedure. A blank worksheet is at "Planning a VPN" on page 7-3.

Table 7-3. 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**
NETBIOS -- Enabled or Disabled:	**Enabled**
Encryption Protocol -- DES or 3DES:	**3DES**
Authentication Protocol -- MD5 or SHA-1:	**SHA-1**
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	**Group 2**
Key Life in seconds:	**28800 (8 hours)**
IKE Life Time in seconds:	**3600 (1 hour)**

VPN Endpoint	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
Client	**toDG834**	**—**	**—**	**Dynamic**
DG834	**toClient**	**192.168.3.1**	**255.255.255.0**	**22.23.24.25**

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

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

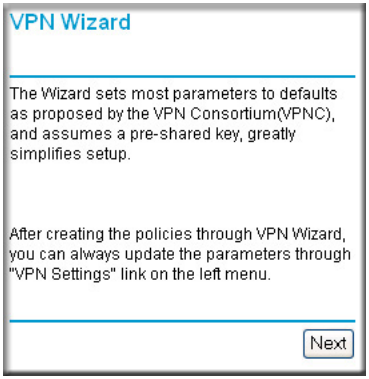


Figure 7-4: VPN Wizard Start Screen

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

   Note: The Connection Name is arbitrary and not relevant to how the configuration functions.

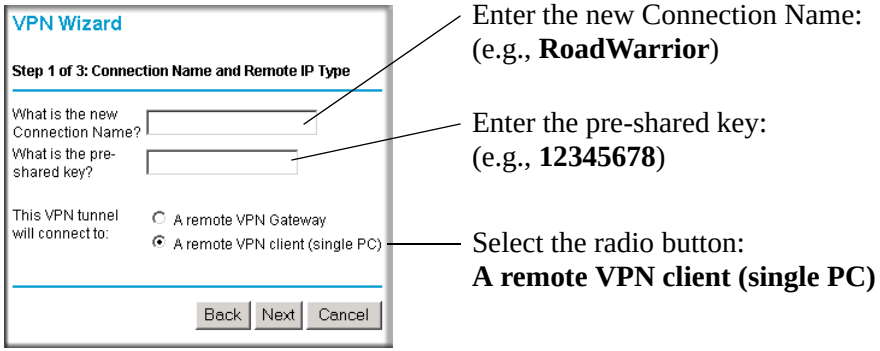


Figure 7-5: Connection Name and Remote IP Type

The Summary screen below displays.

Figure 7-6: VPN Wizard Summary

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the "**here**" link (see Figure 7-6). Click **Back** to return to the Summary screen.

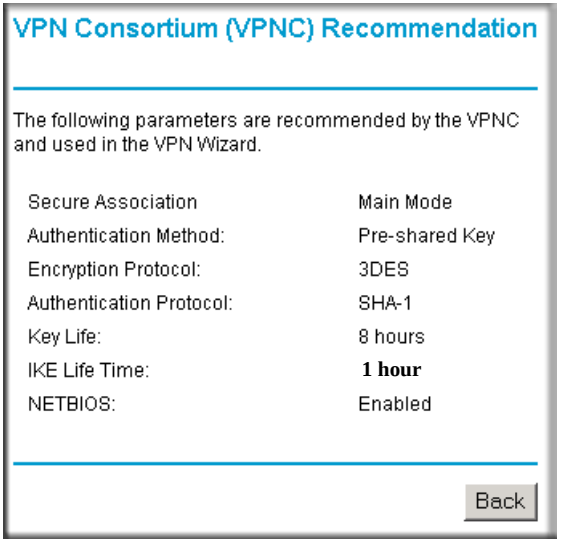


Figure 7-7: VPNC Recommended Settings

3. Click **Done** on the Summary screen (see Figure 7-6) to complete the configuration procedure. The VPN Policies menu below displays showing that the new tunnel is enabled.

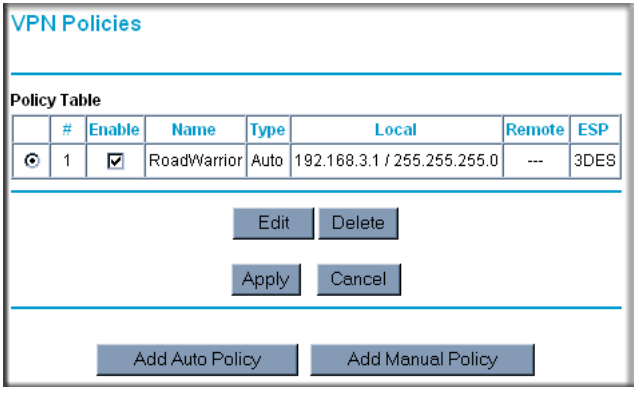


Figure 7-8: VPN Policies

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

Note: Refer to "Using Auto Policy to Configure VPN Tunnels" on page 7-36 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. We will assume the PC running the client has a dynamically assigned IP address.

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

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

1. Install the NETGEAR ProSafe VPN Client on the remote PC and reboot.
   - You may need to insert your Windows CD to complete the installation.
   - If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating "The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed." You can disregard this message.
   - Install the IPSec Component. You may have the option to install either the VPN Adapter or the IPSec Component or both. The VPN Adapter is not necessary.
   - The system should show the ProSafe icon () in the system tray after rebooting.
   - Double-click the system tray icon to open the Security Policy Editor.
2. Add a new connection.
   - Run the NETGEAR ProSafe Security Policy Editor program and, using the "VPN Tunnel Configuration Worksheet" on page 7-8, create a VPN Connection.
   - From the Edit menu of the Security Policy Editor, click Add, then Connection. A "New Connection" listing appears in the list of policies. Rename the "New Connection" so that it matches the Connection Name you entered in the VPN Settings of the DG834 on LAN A.

Note: In this example, the Connection Name used on the client side of the VPN tunnel is **toDG834** and it does not have to match the **RoadWarrior** Connection Name used on the gateway side of the VPN tunnel (see Figure 7-5) because Connection Names are arbitrary to how the VPN tunnel functions.

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

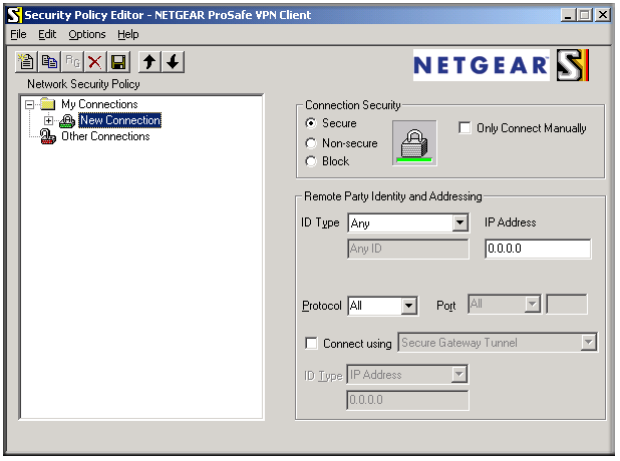


Figure 7-9: Security Policy Editor New Connection

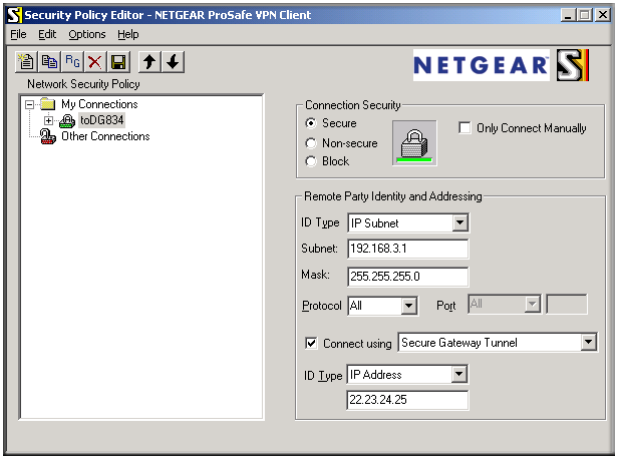


Figure 7-10: Security Policy Editor Connection Settings

- Select the Secure in the Connection Security check box.
- Select IP Subnet in the ID Type menu.

- In this example, type **192.168.3.1** in the Subnet field as the network address of the DG834.
- Enter **255.255.255.0** in the Mask field as the LAN Subnet Mask of the DG834.
- Select All in the Protocol menu to allow all traffic through the VPN tunnel.
- Select the Connect using Secure Gateway Tunnel check box.
- Select IP Address in the ID Type menu below the check box.
- Enter the public WAN IP Address of the DG834 in the field directly below the ID Type menu. In this example, **22.23.24.25** would be used.
- The resulting Connection Settings are shown in Figure 7-10.

3. Configure the Security Policy in the NETGEAR ProSafe VPN Client software.

- In the Network Security Policy list, expand the new connection by double clicking its name or clicking on the "+" symbol. My Identity and Security Policy subheadings appear below the connection name.
- Click on the Security Policy subheading to show the Security Policy menu.

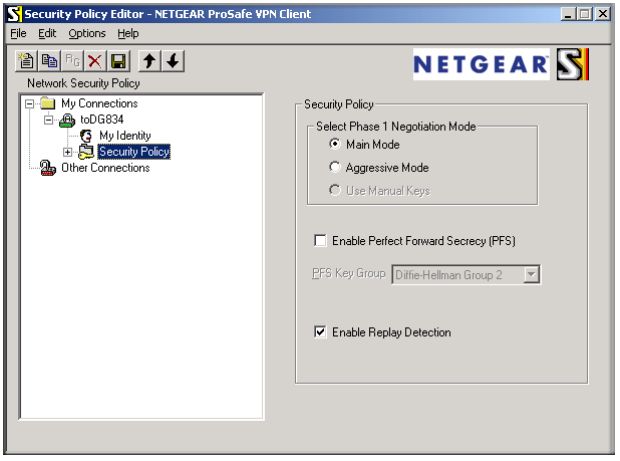


Figure 7-11: Security Policy Editor Security Policy

- Select the Main Mode in the Select Phase 1 Negotiation Mode check box.

4. Configure the VPN Client Identity.

   In this step, you will provide information about the remote VPN client PC. You will need to provide:

   — The Pre-Shared Key that you configured in the DG834.

   — Either a fixed IP address or a "fixed virtual" IP address of the VPN client PC.

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

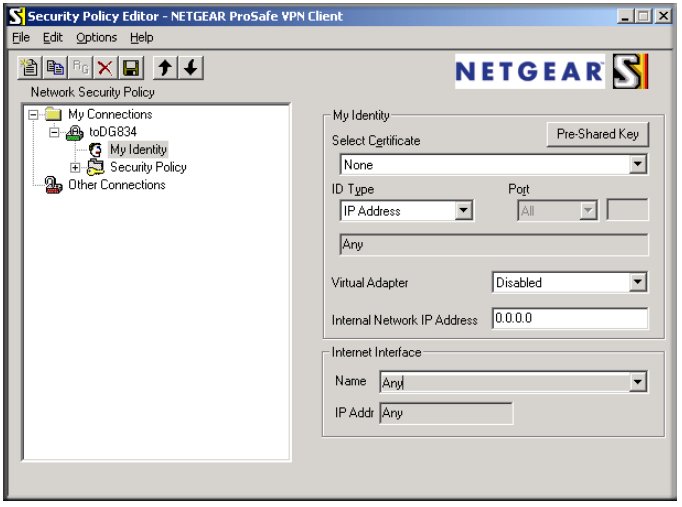


Figure 7-12: Security Policy Editor My Identity

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

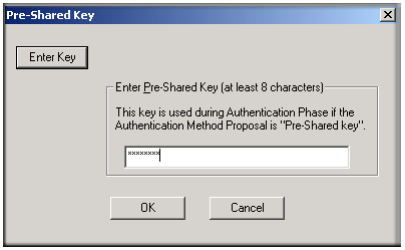


Figure 7-13: Security Policy Editor Pre-Shared Key

5. Configure the VPN Client Authentication Proposal.

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

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

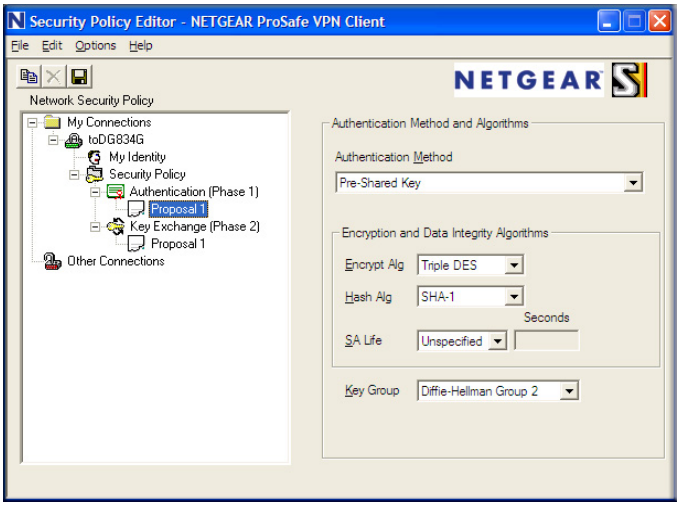


Figure 7-14: Security Policy Editor Authentication

   - In the Authentication Method menu, select Pre-Shared key.
   - In the Encrypt Alg menu, select the type of encryption to correspond with what was configured for the Encryption Protocol in the DG834 in Table 7-3 on page 7-8. In this example, use Triple DES.
   - In the Hash Alg menu, select SHA-1.
   - In the SA Life menu, select Unspecified.
   - In the Key Group menu, select Diffie-Hellman Group 2.

6. Configure the VPN Client Key Exchange Proposal.

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

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

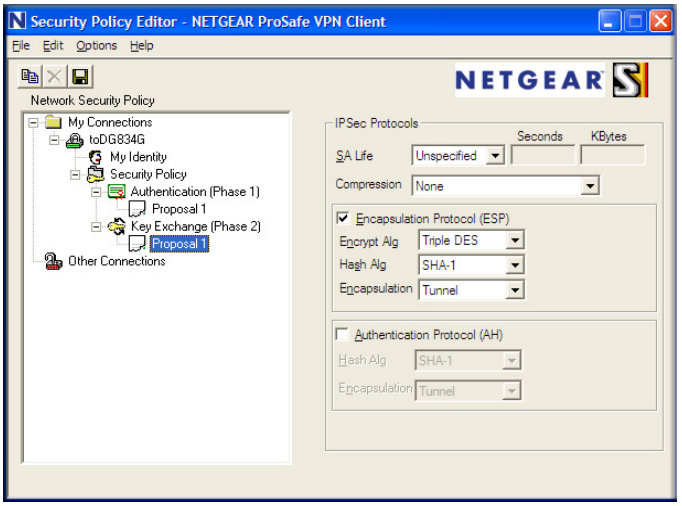


Figure 7-15: Security Policy Editor Key Exchange

- In the SA Life menu, select Unspecified.
- In the Compression menu, select None.
- Check the Encapsulation Protocol (ESP) checkbox.
- In the Encrypt Alg menu, select the type of encryption to correspond with what was configured for the Encryption Protocol in the DG834 in Table 7-3 on page 7-8. In this example, use Triple DES.
- In the Hash Alg menu, select SHA-1.
- In the Encapsulation menu, select Tunnel.
- Leave the Authentication Protocol (AH) checkbox unchecked.

7. Save the VPN Client Settings.

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

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

8. Check the VPN Connection.

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

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

   a. Establish an Internet connection from the PC.

   b. On the Windows taskbar, click the Start button, and then click Run.

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

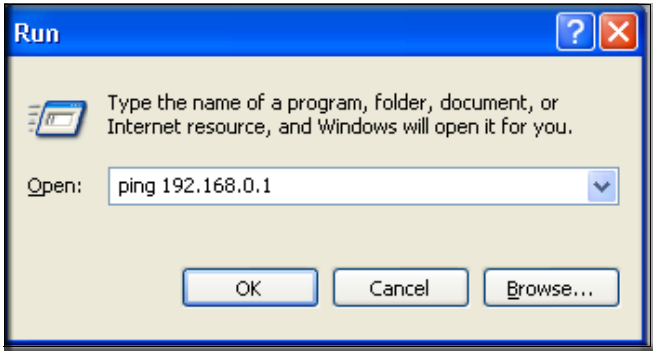


Figure 7-16: Running a Ping test to the LAN from the PC

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

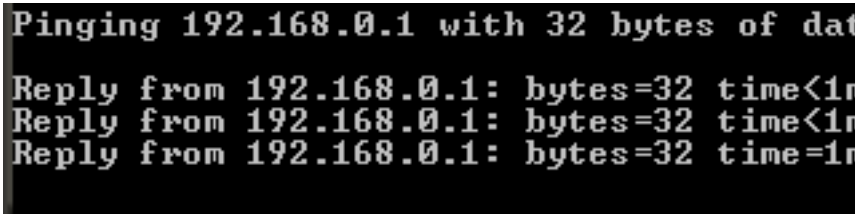


Figure 7-17: Ping test results

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

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

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

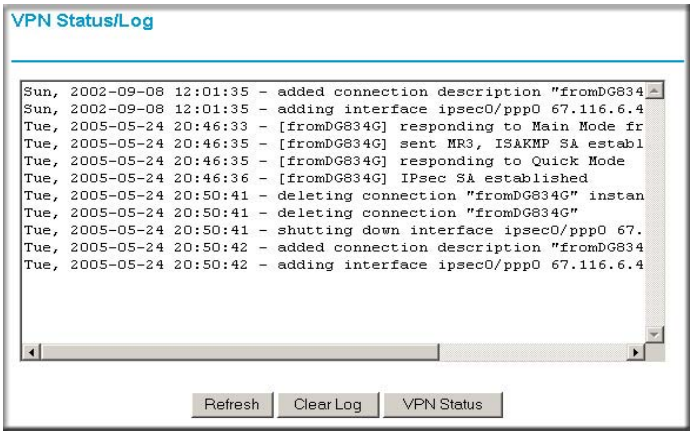


Figure 7-18: Log Viewer screen

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

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

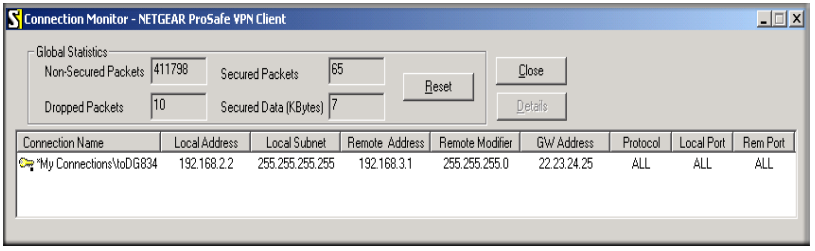


Figure 7-19: Connection Monitor screen

In this example you can see the following:

- The DG834 has a public IP WAN address of 22.23.24.25.

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

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

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

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

Note: This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in Table 7-2 on page 7-5. If you have special requirements not covered by these VPNC-recommended parameters, refer to “How to Set Up VPN Tunnels in Special Circumstances” on page 7-35 to set up the VPN tunnel.

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

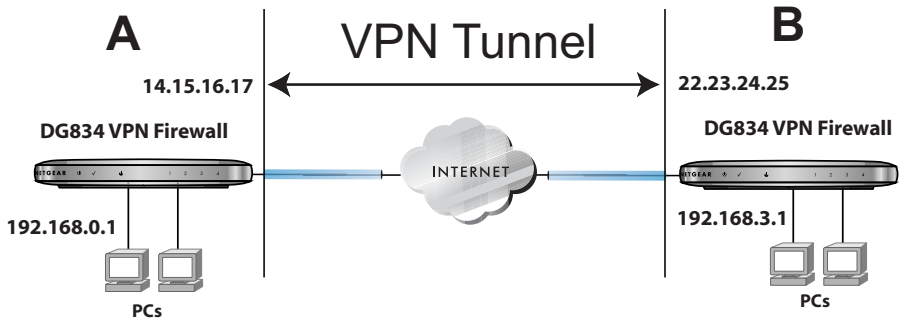


Figure 7-20: Gateway-to-Gateway VPN Tunnel

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

Table 7-4. 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**
NETBIOS -- Enabled or Disabled:	**Enabled**
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)
DG834_A	**GW_A**	**192.168.0.1**	**255.255.255.0**	**14.15.16.17**
DG834_B	**GW_B**	**192.168.3.1**	**255.255.255.0**	**22.23.24.25**

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

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

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

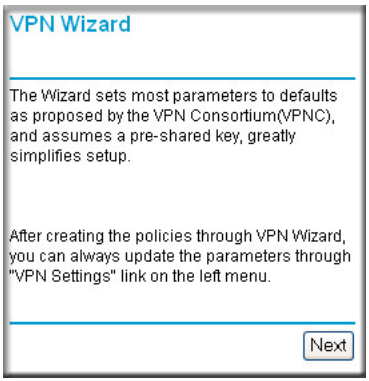


Figure 7-21: VPN Wizard Start Screen

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

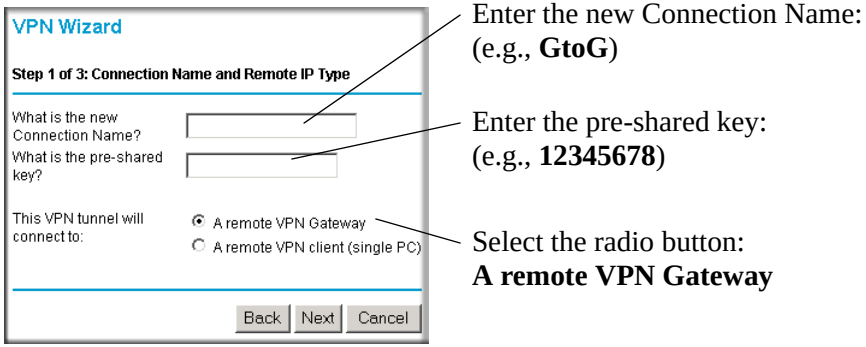
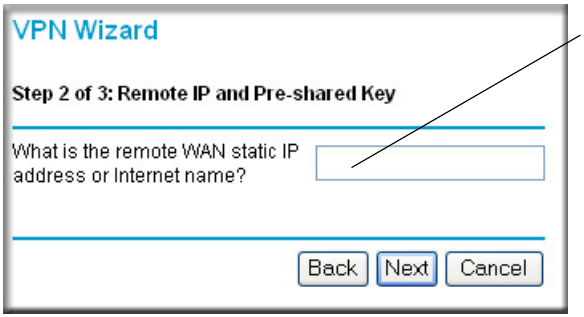


Figure 7-22: Connection Name and Remote IP Type

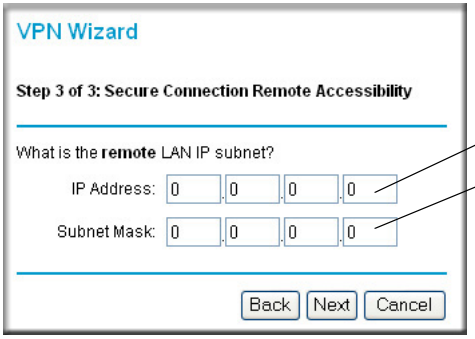
3. Fill in the IP Address or FQDN for the target VPN endpoint WAN connection and click **Next**.



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

Figure 7-23: Remote IP

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



Enter the LAN IP settings of the remote VPN gateway:

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

Figure 7-24: Secure Connection Remote Accessibility

The Summary screen below displays.

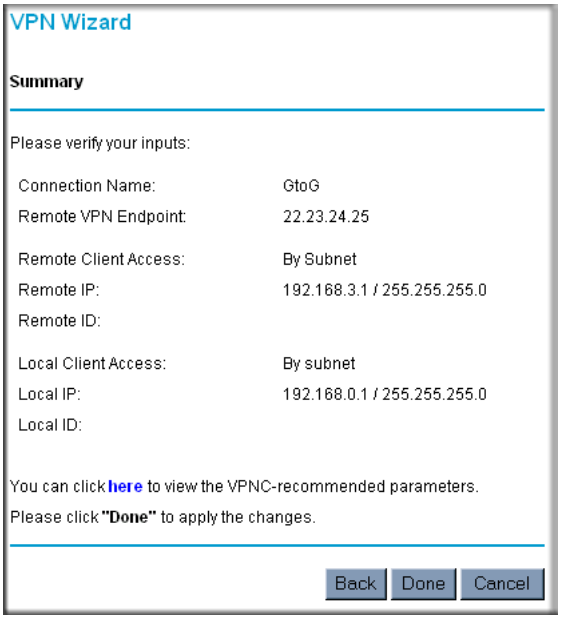


Figure 7-25: VPN Wizard Summary

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the "**here**" link (see Figure 7-25). Click **Back** to return to the Summary screen.

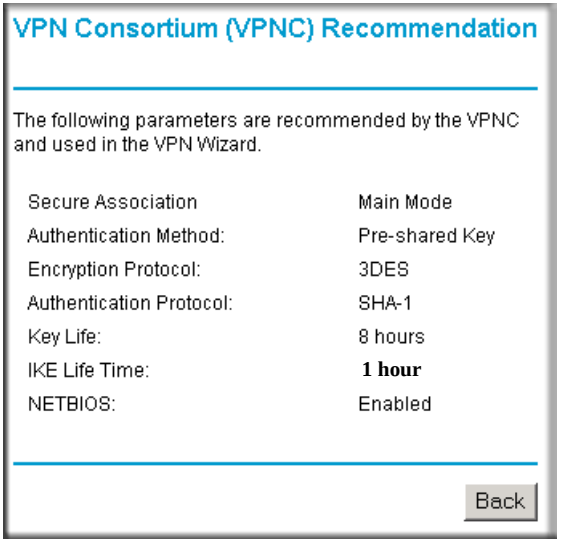


Figure 7-26: VPN Recommended Settings

5. Click **Done** on the Summary screen (see Figure 7-25) to complete the configuration procedure. The VPN Settings menu below displays showing that the new tunnel is enabled.

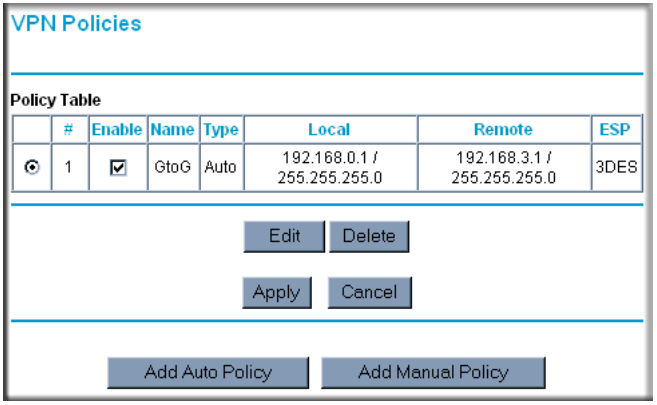


Figure 7-27: VPN Policies

Note: Refer to "Using Auto Policy to Configure VPN Tunnels" on page 7-36 to enable the IKE keepalive capability on an existing VPN tunnel.

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

Note: The VPN Status screen is only one of three ways to active a VPN tunnel. See "Activating a VPN Tunnel" on page 7-27 for information on the other ways.

   a. Open the DG834 management interface and click on VPN Status to get the VPN Status/ Log screen (Figure 7-28).

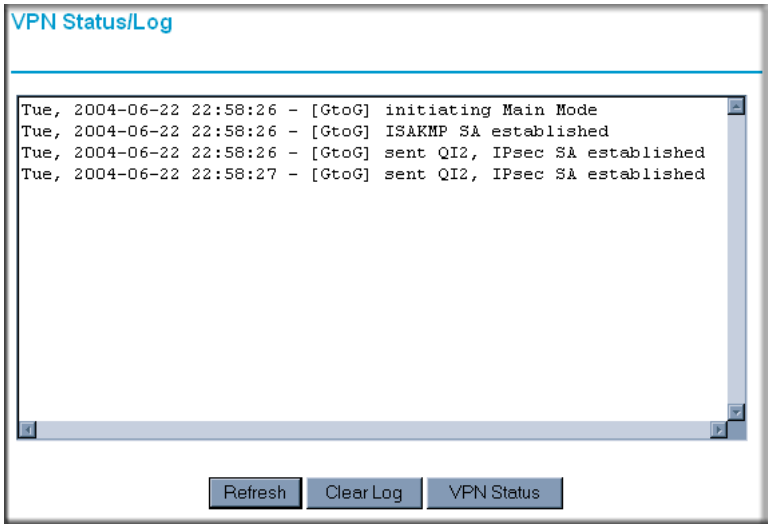


Figure 7-28: VPN Status/Log Screen

   b. Click on VPN Status (Figure 7-30) to get the Current VPN Tunnels (SAs) screen (Figure 7-29). Click on Connect for the VPN tunnel you want to activate.

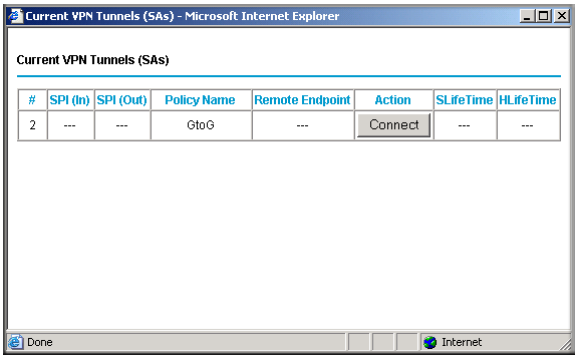


Figure 7-29: Current VPN Tunnels (SAs) Screen

c. Look at the VPN Status/Log screen (Figure 7-28) to verify that the tunnel is connected.

VPN Tunnel Control

Activating a VPN Tunnel

There are three ways to activate a VPN tunnel:

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

Note: Refer to "Using Auto Policy to Configure VPN Tunnels" on page 7-36 to enable the IKE keepalive capability on an existing VPN tunnel.

Using the VPN Status Page to Activate a VPN Tunnel

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

1. Log in to the Router.
2. Open the DG834 management interface and click on VPN Status to get the VPN Status/Log screen (Figure 7-30).

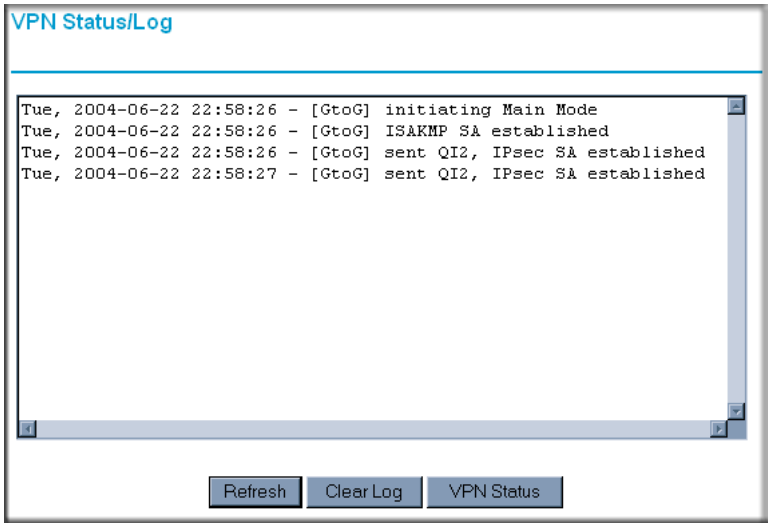


Figure 7-30: VPN Status/Log Screen

3. Click on VPN Status (Figure 7-30) to get the Current VPN Tunnels (SAs) screen (Figure 7-31). Click on Connect for the VPN tunnel you want to activate.

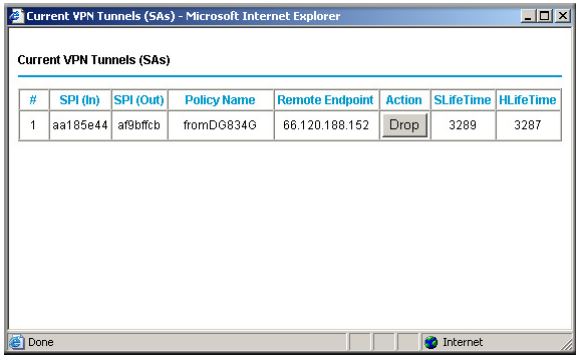


Figure 7-31: Current VPN Tunnels (SAs) Screen

Activate the VPN Tunnel by Pinging the Remote Endpoint

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

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

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

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

  a. Establish an Internet connection from the PC.

  b. On the Windows taskbar, click the Start button, and then click Run.

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

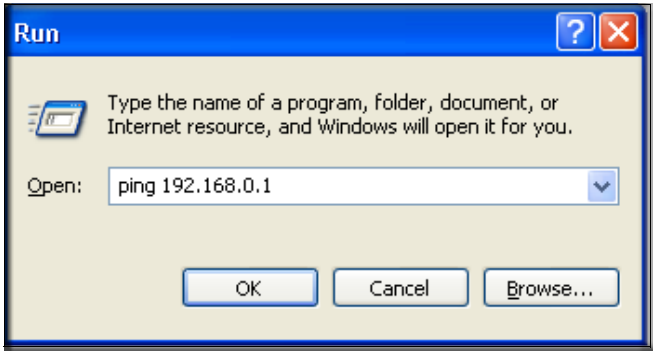


Figure 7-32: Running a Ping test to the LAN from the PC

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

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

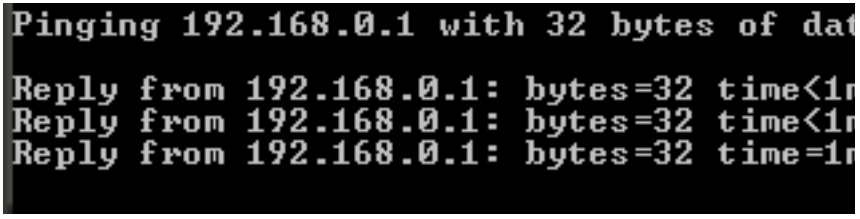


Figure 7-33: Ping test results

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

- **Gateway-to-Gateway Configuration**—test the VPN tunnel by pinging the remote network from a PC attached to the DG834.

  a. Open command prompt (i.e., Start -> Run -> cmd).

  b. ping 192.168.3.1.

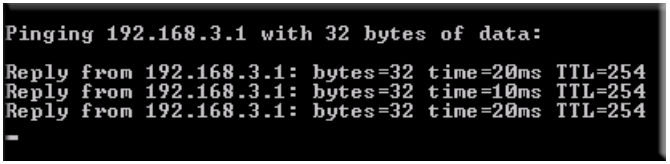


Figure 7-34: Pinging test results

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

Start Using a VPN Tunnel to Active It

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

Verifying the Status of a VPN Tunnel

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

1. Log in to the Router.
2. Open the DG834 management interface and click on VPN Status to get the VPN Status/Log screen (Figure 7-35).

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

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

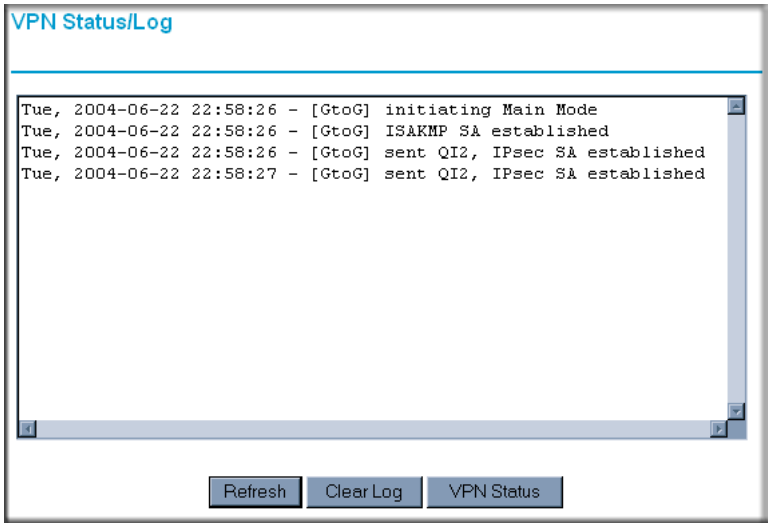


Figure 7-35: VPN Status/Log Screen

3. Click on VPN Status (Figure 7-30) to get the Current VPN Tunnels (SAs) screen (Figure 7-31).

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

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

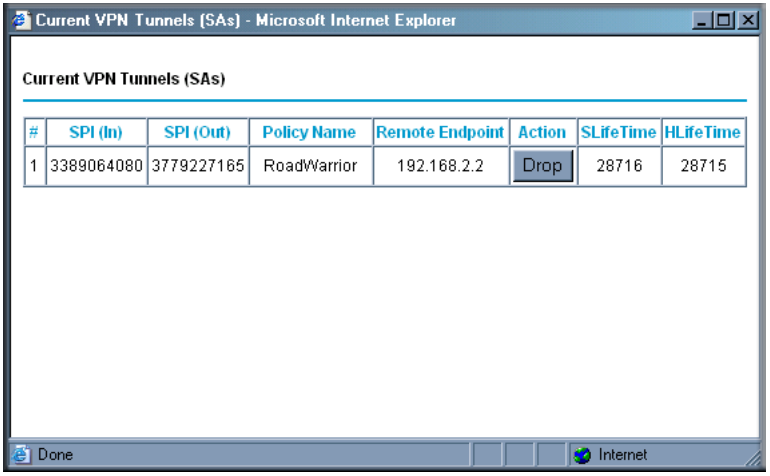


Figure 7-36: Current VPN Tunnels (SAs) Screen

Deactivating a VPN Tunnel

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

- Policy table on VPN Policies page
- VPN Status page

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

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

1. Log in to the Router.
2. Open the DG834 management interface and click on VPN Policies to get the VPN Policies screen (Figure 7-38).

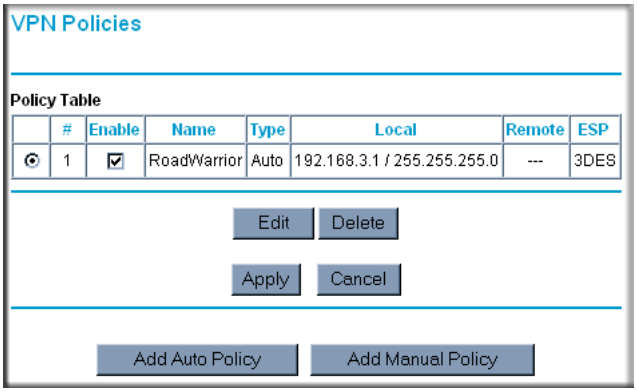


Figure 7-37: VPN Policies

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

Using the VPN Status Page to Deactivate a VPN Tunnel

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

1. Log in to the Router.
2. Open the DG834 management interface and click on VPN Status to get the VPN Status/Log screen (Figure 7-38).

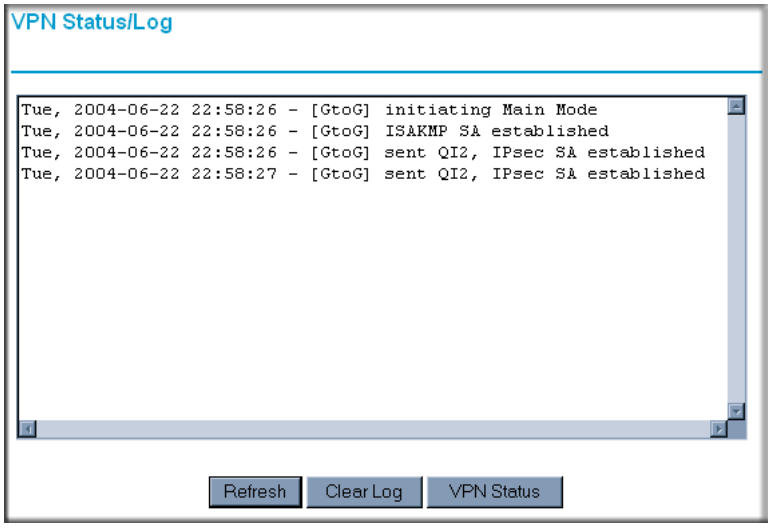


Figure 7-38: VPN Status/Log Screen

3. Click VPN Status (Figure 7-38) to get the Current VPN Tunnels (SAs) screen (Figure 7-39). Click Drop for the VPN tunnel you want to deactivate.

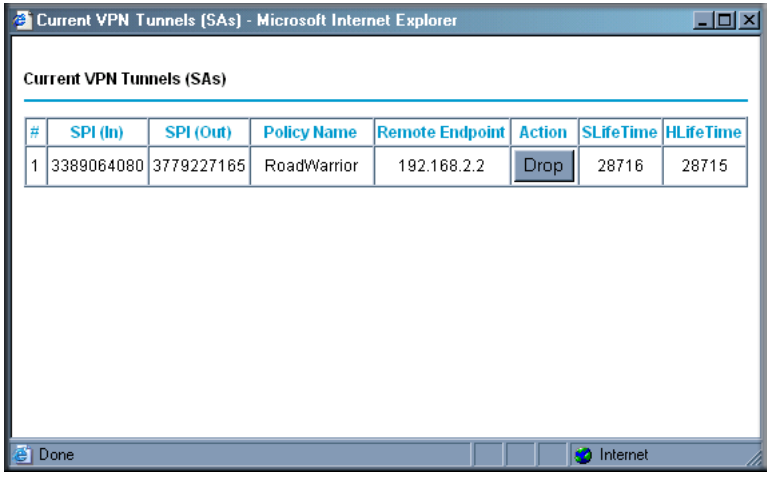


Figure 7-39: Current VPN Tunnels (SAs) Screen

Note: When NETBIOS is enabled (which it is in the VPNC defaults implemented by the VPN Wizard), automatic traffic will reactivate the tunnel. To prevent reactivation from happening, either disable NETBIOS or disable the policy for the tunnel (see "Using the Policy Table on the VPN Policies Page to Deactivate a VPN Tunnel" on page 7-32).

Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the Router.
2. Open the DG834 management interface and click VPN Policies to display the VPN Policies screen (Figure 7-40). Select the radio button for the VPN tunnel to be deleted and click the Delete button.

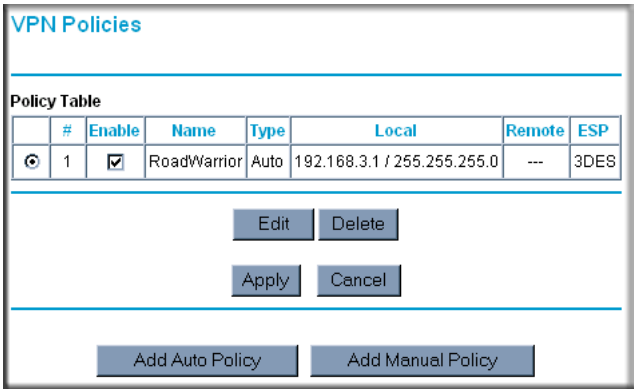


Figure 7-40: VPN Policies

How to Set Up VPN Tunnels in Special Circumstances

When the VPN Wizard and its VPNC defaults (see Table 7-2) are not appropriate for your special circumstances, use one of the following alternatives:

- **Auto Policy**—for a typical automated Internet Key Exchange (IKE) setup, see "Using Auto Policy to Configure VPN Tunnels" on page 7-36. Auto Policy uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys.

- **Manual Policy**—for a Manual Keying setup in which you must specify each phase of the connection, see "Using Manual Policy to Configure VPN Tunnels" on page 7-48. Manual Policy does not use IKE. Rather, you manually enter all the authentication and key parameters. You have more control over the process, however the process is more complex and there are more opportunities for errors or configuration mismatches between your DG834 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 7-41 for an example of using Auto Policy.

Configuring VPN Network Connection Parameters

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

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

Click the VPN Policies link of the main menu, and then click the Add Auto Policy button to display the VPN - Auto Policy menu shown in Figure 7-41.

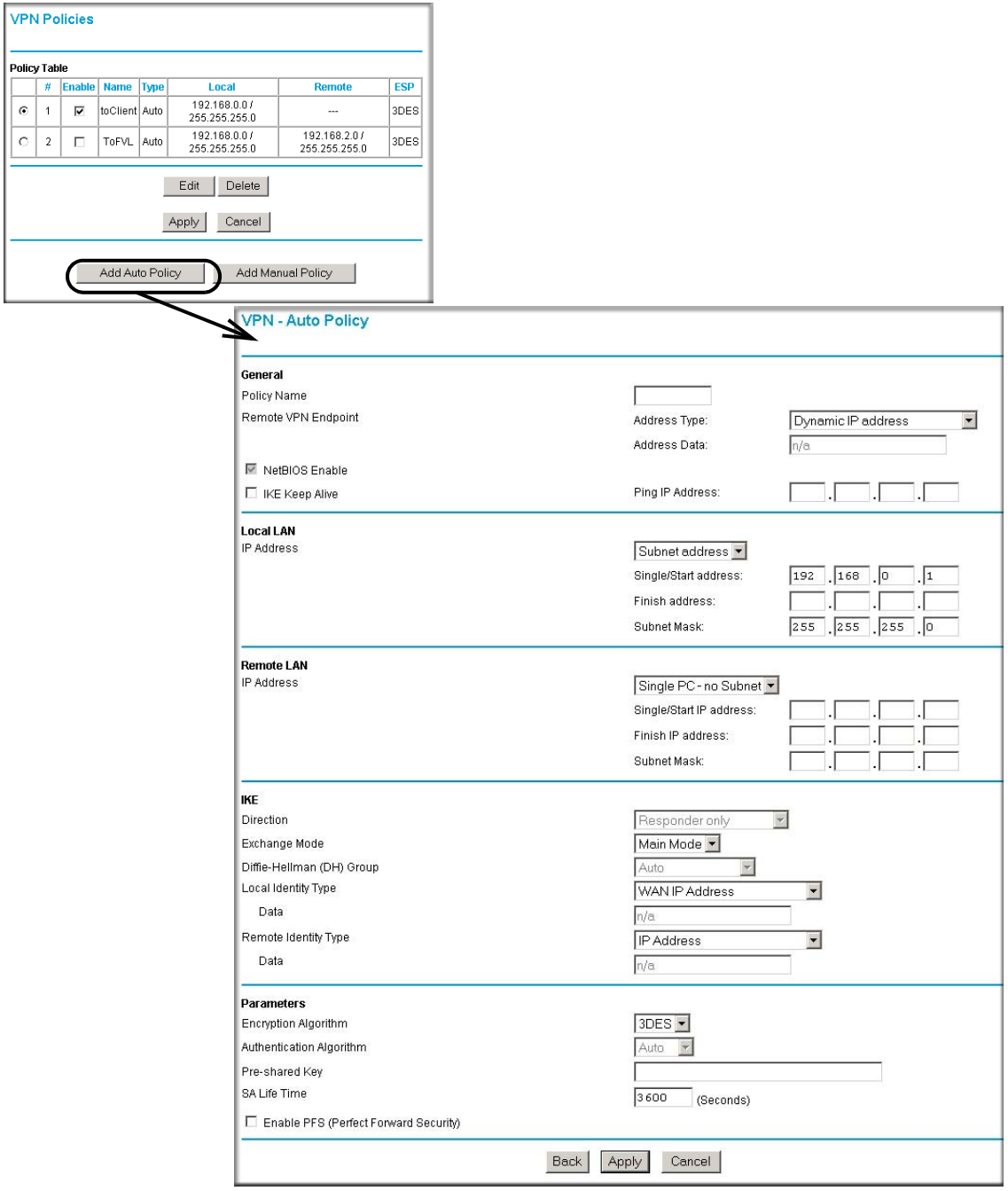


Figure 7-41: DG834 VPN Tunnel Auto Policy Configuration Menu

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

General

These settings identify this policy and determine its major characteristics.

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

  Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".
- **NETBIOS Enable**—check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.
- **IKE Keep-alive**—Enable this if you wish to ensure that a connection is kept open, or, if that is not possible, that it is quickly re-established when disconnected.

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

Local LAN

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

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

Remote LAN

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

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

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

IKE

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

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

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

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

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

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

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

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

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

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

Parameters

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

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

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

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

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

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

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

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

Example of Using Auto Policy

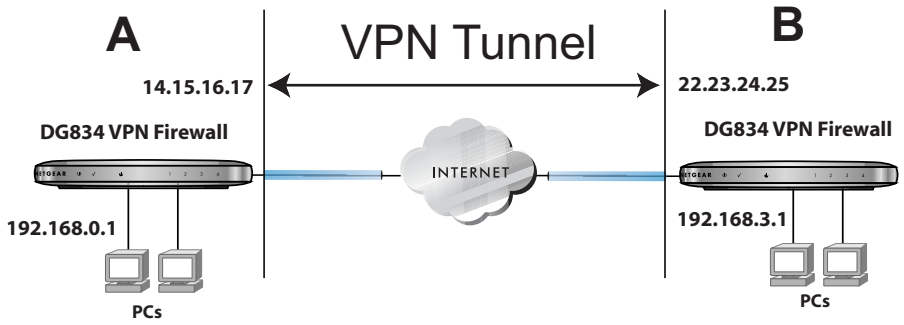


Figure 7-42: Gateway-to-Gateway VPN Tunnel

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

Table 7-1. VPN Tunnel Configuration Worksheet

Connection Name:	**GtoG**
Pre-Shared Key:	**12345678**
Secure Association -- Main Mode or Manual Keys:	**Main**
Perfect Forward Secrecy -- Enabled or Disabled:	**Disabled**
NETBIOS -- Enabled or Disabled:	**Enabled**
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)
DG834 A	**LAN_A**	**192.168.0.1**	**255.255.255.0**	**14.15.16.17**
DG834 B	**LAN_B**	**192.168.3.1**	**255.255.255.0**	**22.23.24.25**

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

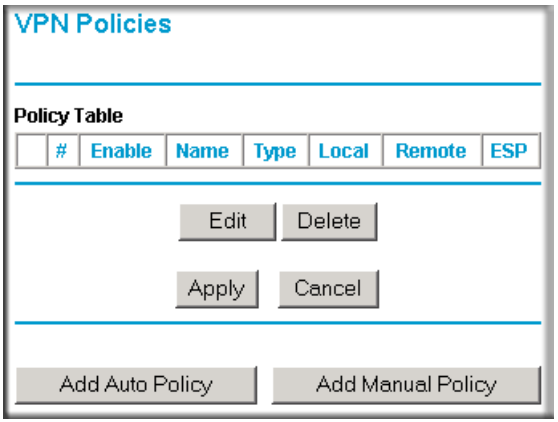


Figure 7-43: VPN Policies Screen

3. Click Add Auto Policy.
4. Enter policy settings (see Figure 7-44).
   - General
     - Policy Name = GtoG
     - Remote VPN Endpoint Address Type = Fixed IP Address
     - Remote VPN Endpoint Address Data = 22.23.24.25
   - Local LAN – use default setting
   - Remote LAN
     - IP Address = select Subnet address from the pulldown menu.
     - Start IP address = 192.168.3.1
     - Subnet Mask = 255.255.255.0
   - IKE
     - Direction = Initiator and Responder
     - Exchange Mode = Main Mode
     - Diffie-Hellman (DH) Group = Group 2 (1024 Bit)
     - Local Identity Type = use default setting

  - Remote Identity Type = use default setting
- Parameters
  - Encryption Algorithm = 3DES
  - Authentication Algorithm = MD5
  - Pre-shared Key = 12345678

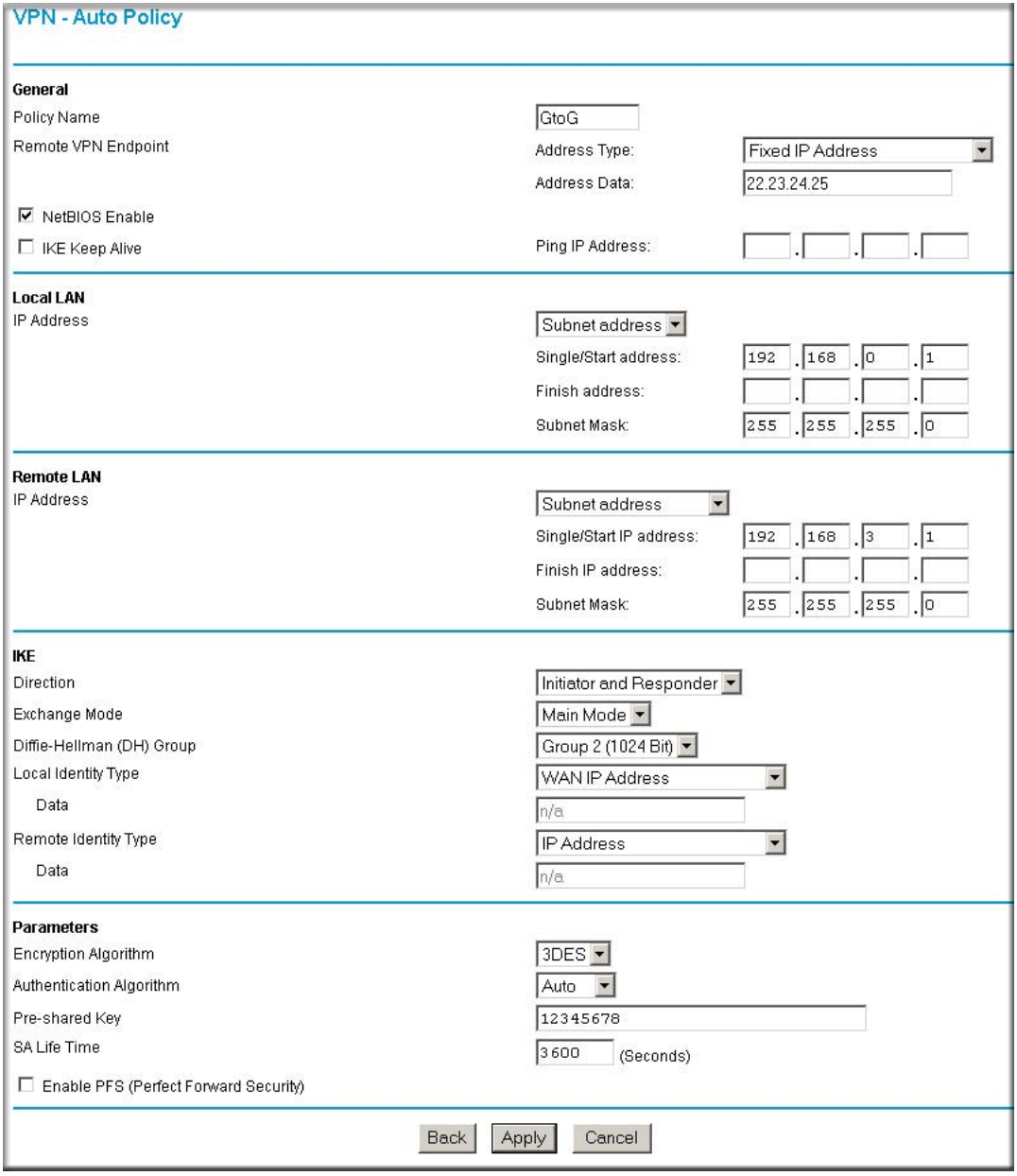


Figure 7-44: VPN Auto Policies Screen

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

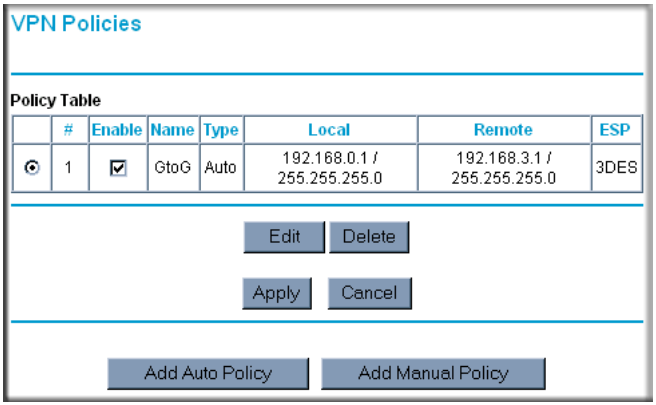


Figure 7-45: VPN Policies Screen

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

Note: The VPN Status screen is only one of three ways to active a VPN tunnel. See "Activating a VPN Tunnel" on page 7-27 for information on the other ways.

   a. Open the DG834 management interface and click on VPN Status to display the VPN Status/Log screen (Figure 7-46).

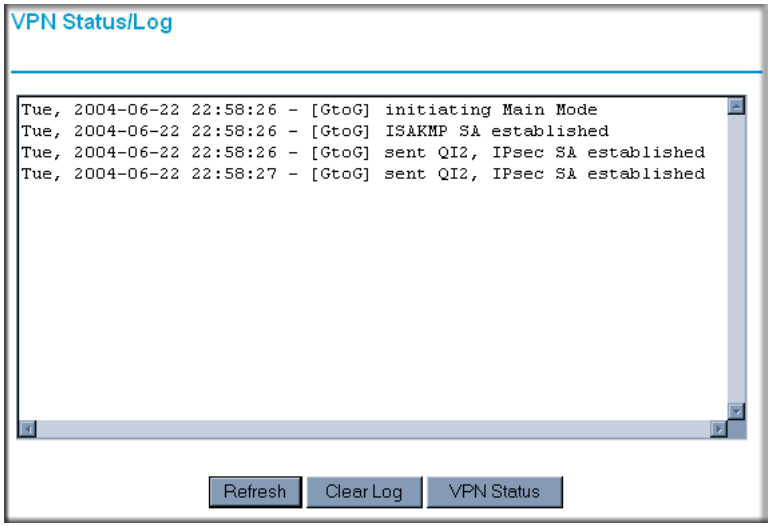


Figure 7-46: VPN Status/Log Screen

b. Click VPN Status (Figure 7-46) to display the Current VPN Tunnels (SAs) screen (Figure 7-47). Click on Connect for the VPN tunnel you want to activate.

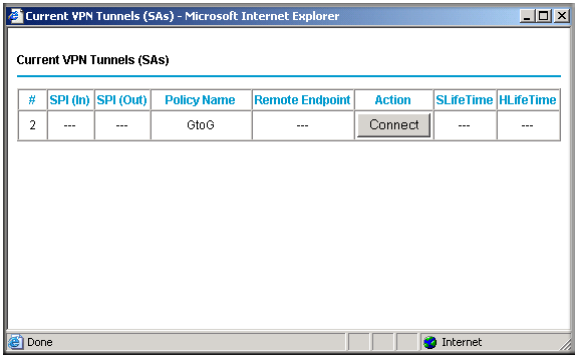


Figure 7-47: Current VPN Tunnels (SAs) Screen

c. Review the VPN Status/Log screen (Figure 7-46) to verify that the tunnel is connected.

Using Manual Policy to Configure VPN Tunnels

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

Click the VPN Policies link of the main menu, and then click the Add Manual Policy radio button to display the Manual Keys menu shown in Figure 7-48.

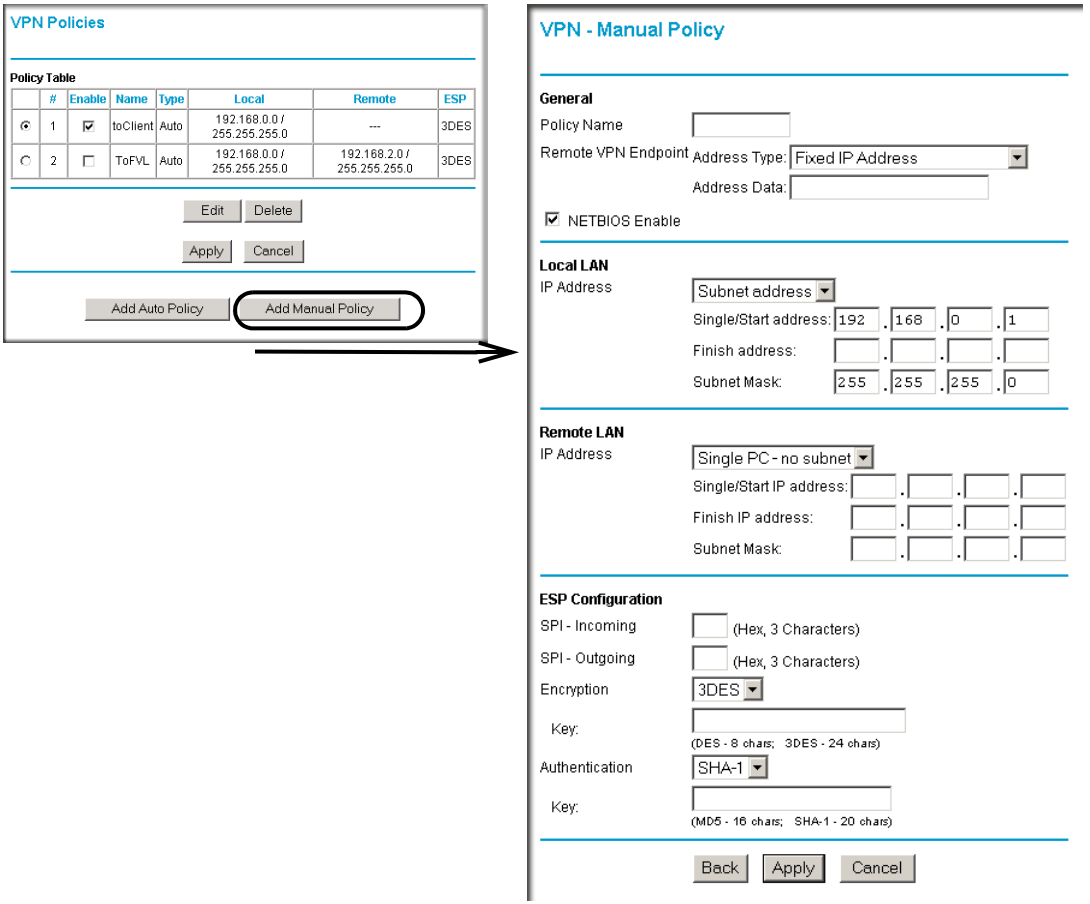


Figure 7-48: DG834 VPN Tunnel Manual Policy Configuration Menu

General

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

- **Policy Name**—enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**—select the desired option (IP address or Fully Qualified Domain Name) and enter the address of the remote VPN endpoint to which you wish to connect.

  Note: The remote VPN endpoint must have this VPN Gateway's address entered as its "Remote VPN Endpoint".
- **NETBIOS Enable**—check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking.

Local LAN

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

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

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

Remote LAN

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

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

- **Range address**—enter the starting IP address in the "Single/Start IP address" field, and the finish IP address in the "Finish IP address" field. This must be an address range used on the remote LAN.
- **Subnet address**—enter an IP address in the "Single/Start IP address" field, and the desired network mask in the "Subnet Mask" field.

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

ESP Configuration

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

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

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

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

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

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

Chapter 8
Troubleshooting

This chapter gives information about troubleshooting your DG834 ADSL Firewall 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 8-1.
- I can't access the router's configuration with my browser.

  Go to "Troubleshooting the Web Configuration Interface" on page 8-3.
- I've configured the router but I can't access the Internet.

  Go to "Troubleshooting the ISP Connection" on page 8-4.
- I can't remember the router's configuration password.
- I want to clear the configuration and start over again.

  Go to "Restoring the Default Configuration and Password" on page 8-9.

Basic Functioning

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

1. When power is first applied, verify that the Power LED is on (see "The Router's Front Panel" on page 2-5 for an illustration and explanation of the LEDs).
2. Verify that the Test LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 10 seconds, verify that:
   a. The Test LED is not lit.
   b. The LAN port LEDs are lit for any local ports that are connected.
   c. The WAN port LED is lit.

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

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

Power LED Not On

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

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

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

Test LED Never Turns On or Test LED Stays On

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

If you experience problems with the Test LED:

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

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

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

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

LAN or WAN Port LEDs Not On

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

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

- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
  - When connecting the router's WAN ADSL port, use the cable that was supplied with the DG834.

Troubleshooting the Web Configuration Interface

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to "Verifying TCP/IP Properties" on page C-6 or "Verifying TCP/IP Properties for Macintosh Computers" on page C-17 to find your computer's IP address. Follow the instructions in Appendix C to configure your computer.

  Note: If your computer's IP address is shown as 169.254.x.x:
  Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.
- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Using the Reset button" on page 8-9.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

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

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

Troubleshooting the ISP Connection

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

ADSL link

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

WAN LED Green or Blinking Green

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

WAN LED Blinking Yellow

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

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

If disconnecting telephones does not result in a green WAN 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.

WAN LED Off

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

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

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It may be necessary to use a swapper if you ADSL signal is on pins 1 and 4 or the RJ-11 jack. The DG834 ADSL router uses pins 2 and 3.

Obtaining a WAN IP Address

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

To check the WAN IP address from the browser interface:

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

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

- Your ISP may require a Multiplexing Method or Virtual Path Identifier/Virtual Channel Identifier parameter.
  Verify with your ISP the Multiplexing Method and parameter value, and update the router's ADSL Settings accordingly.
- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or PPP over ATM (PPPOA) login.
- If you have selected a login program, you may have incorrectly set the Service Name, User Name and Password. See "Troubleshooting PPPoE or PPPoA", below.
- Your ISP may check for your computer's host name.
  Assign the computer Host Name of your ISP account to the router in the browser-based Setup Wizard.

- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:

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

  OR

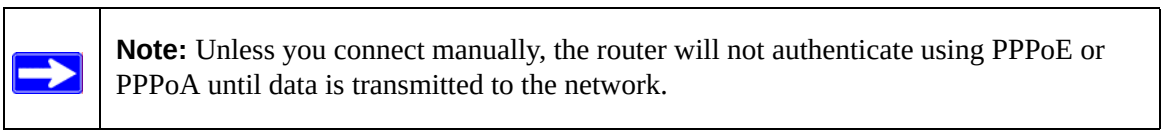
  Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu. Refer to "Manually Configuring Your Internet Connection" on page 3-14.

Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

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

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



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

Troubleshooting Internet Browsing

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

- Your computer may not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address as described in "Verifying TCP/IP Properties" on page C-6. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

  If your computer obtains its information from the router by DHCP, reboot the computer and verify the router address as described in "Verifying TCP/IP Properties" on page C-6.

Troubleshooting a TCP/IP Network Using the Ping Utility

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

Testing the LAN Path to Your Router

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

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

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

   `ping 192.168.0.1`
3. Click OK.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

   `Request timed out`

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

- Wrong physical connections
  - — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or WAN Port LEDs Not On" on page 8-2.
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - — Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

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

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

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

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

- — Check that your PC has the IP address of your router listed as the default router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default router as described in "Verifying TCP/IP Properties" on page C-6.
- — Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- — Check that your cable or DSL modem is connected and functioning.
- — If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- — Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC. Refer to "Manually Configuring Your Internet Connection" on page 3-14.

Restoring the Default Configuration and Password

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

- Use the Erase function of the Web Configuration Manager (see "Backing Up, Restoring, or Erasing Your Settings" on page 5-1).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

Using the Reset button

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

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

Problems with Date and Time

The E-mail menu in the Content Filtering section displays the current date and time of day. The DG834 ADSL router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

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

Appendix A
Technical Specifications

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

Network Protocol and Standards Compatibility

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

Power Adapter

North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	15 V AC @ 1.0A output, 30W maximum

Physical Specifications

Dimensions:	10" x 6.7" x 1.3" 255 mm x 169 mm x 34 mm
Weight:	1.4 lbs. 0.62 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, Dual RJ-11, pins 2 and 3 T1.413, G.DMT, G.Lite ITU Annex A or B

Appendix B
Network and Routing Basics

This chapter provides an overview of IP networks and routing.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The DG834 ADSL Firewall Router is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The DG834 ADSL router supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

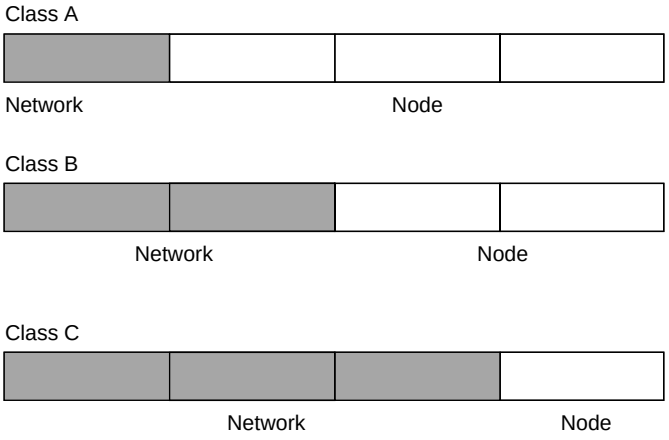


Figure 8-1: Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  `1.x.x.x to 126.x.x.x.`

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  `128.1.x.x to 191.254.x.x.`

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  `192.0.1.x to 223.255.254.x.`

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  `224.0.0.0 to 239.255.255.255.`

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

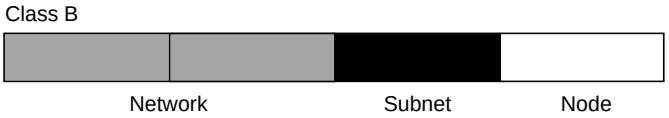


Figure 8-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

	**Note:** The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table 8-1. Netmask Notation Translation Table for One Octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table 8-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the DG834 ADSL router is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at www.ietf.org.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The DG834 ADSL router employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.

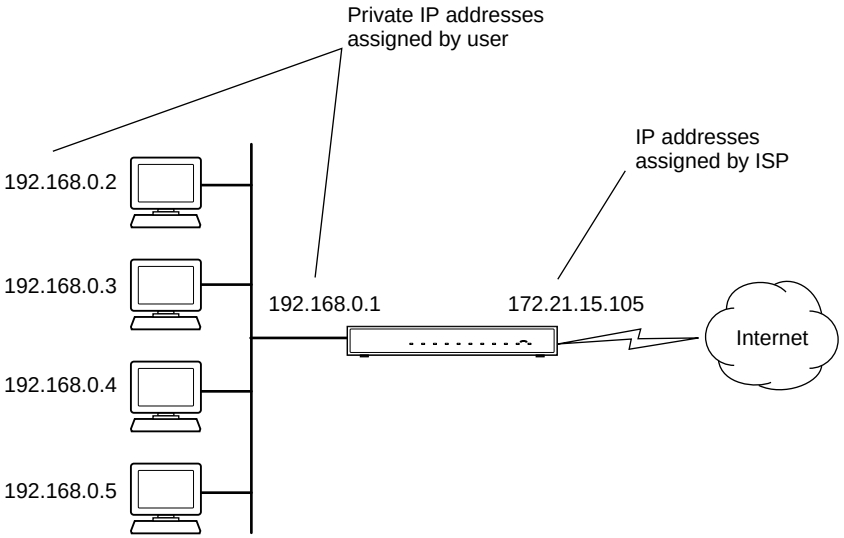


Figure 8-3: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets,* and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com.* This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The DG834 ADSL router has the capacity to act as a DHCP server.

The DG834 ADSL router also functions as a DHCP client when connecting to the ISP. The router can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection states. Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring as described below in Table B-1

Table B-1. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Category 5 Cable Quality

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

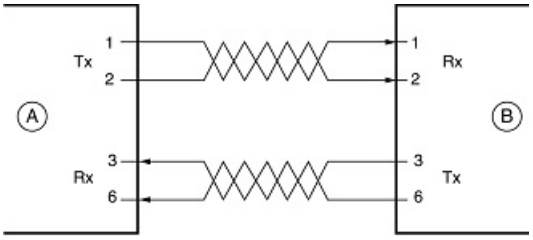
The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Inside Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

Figure B-1 illustrates straight-through twisted pair cable.



Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-1: Straight-Through Twisted-Pair Cable

Figure B-2 illustrates crossover twisted pair cable.

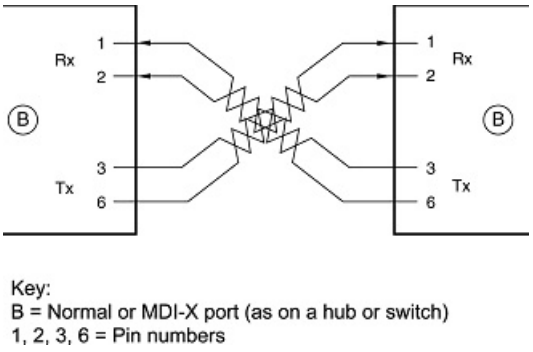


Figure B-2: Crossover Twisted-Pair Cable

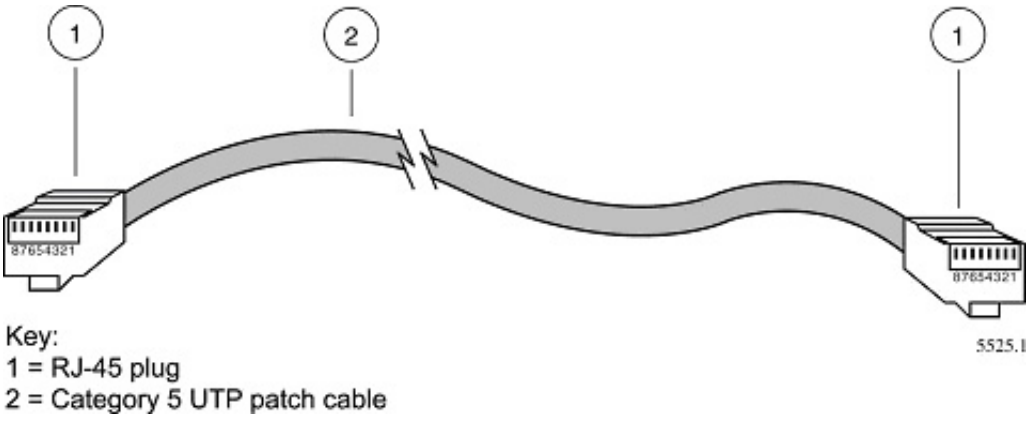


Figure B-3: Category 5 UTP Cable with Male RJ-45 Plug at Each End

Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

The DG834 ADSL router incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

Appendix C
Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the DG834 ADSL Firewall Router and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

Note: If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your router. Write down this information before reconfiguring your computers. Refer to "Obtaining ISP Configuration Information for Windows Computers" on page C-19 or "Obtaining ISP Configuration Information for Macintosh Computers" on page C-20 for further information.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/ IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/ IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.
- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each PC and the router must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to "Appendix B, "Network and Routing Basics."

The DG834 ADSL router is shipped preconfigured as a DHCP server. The router assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254
- Subnet mask—255.255.255.0
- Gateway address (the router)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

Configuring Windows 95, 98, and Me for TCP/IP Networking

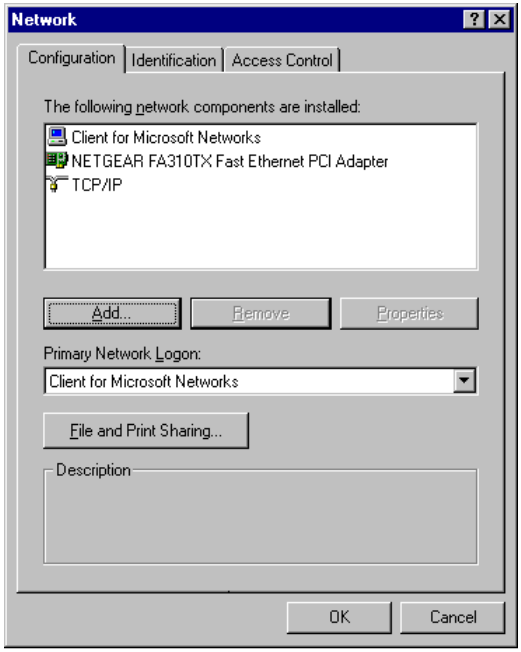
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Installing or Verifying Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:



You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

Note: It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

a. Click the Add button.

b. Select Adapter, and then click Add.

c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

a. Click the Add button.

b. Select Client, and then click Add.

c. Select Microsoft.

d. Select Client for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 95B, 98, and Me

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

1

Locate your **Network Neighborhood** icon.

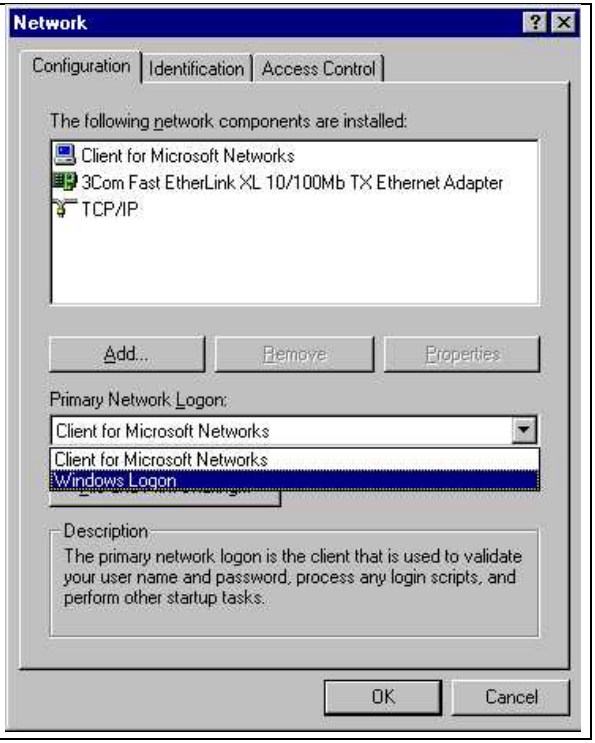
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click **Start** on the task bar located at the bottom left of the window.
  - Choose **Settings**, and then **Control Panel**.
  - Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

2

Verify the following settings as shown:

- Client for Microsoft Network exists
- Ethernet adapter is present
- TCP/IP is present
- **Primary Network Logon** is set to Windows logon

Click on the **Properties** button. The following TCP/IP Properties window will display.



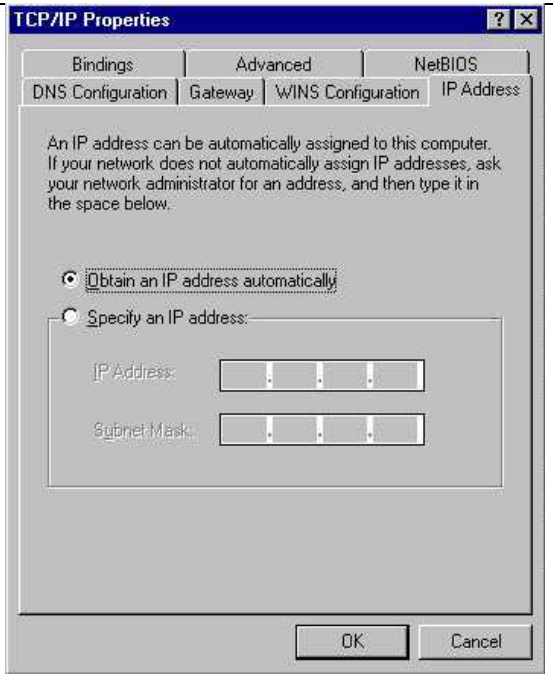
3

- By default, the **IP Address** tab is open on this window.
- Verify the following:

  Obtain an IP address automatically is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.
- Click **OK** to continue.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



Selecting the Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.
4. Select "I want to connect through a Local Area Network" and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.

2. Type **winipcfg**, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

Configuring Windows NT4, 2000 or XP for IP Networking

As part of the PC preparation process, you may need to install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Installing or Verifying Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.
6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Then, restart your PC.

DHCP Configuration of TCP/IP in Windows XP, 2000, or NT4

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

DHCP Configuration of TCP/IP in Windows XP

1

Locate your **Network Neighborhood** icon.

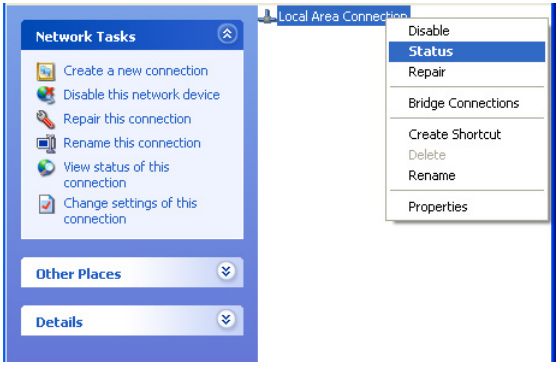
- Select **Control Panel** from the Windows XP new Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

2

- Now the Network Connection window displays.

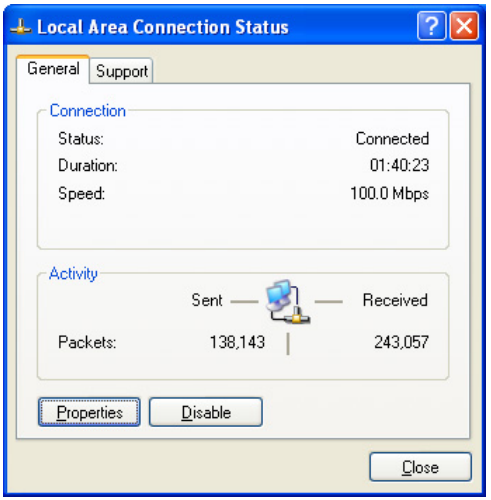
  The Connections List that shows all the network connections set up on the PC, located to the right of the window.

- Right-click on the **Connection** you will use and choose **Status**.



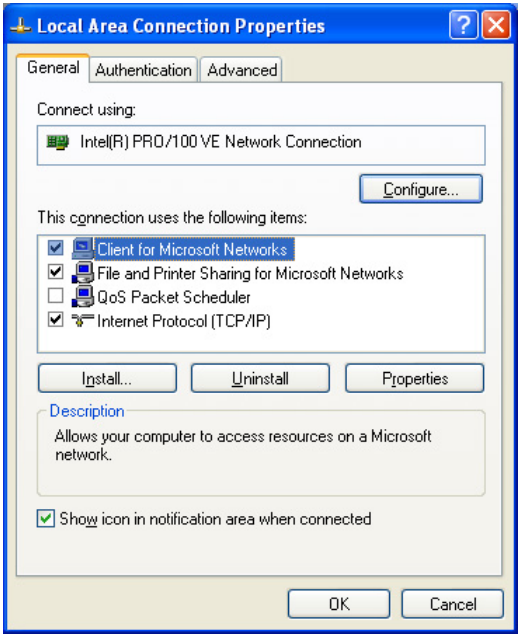
3

- Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.
- Administrator logon access rights are needed to use this window.
- Click the **Properties button** to view details about the connection.



4

- The TCP/IP details are presented on the Support tab page.
- Select **Internet Protocol,** and click **Properties** to view the configuration information**.**

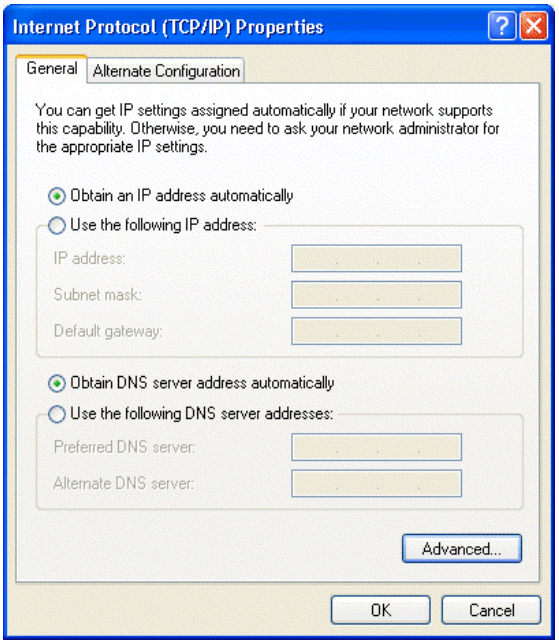


5

- Verify that the **Obtain an IP address automatically** radio button is selected.
- Verify that **Obtain DNS server address automatically** radio button is selected.
- Click the **OK** button.

This completes the DHCP configuration of TCP/IP in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.



DHCP Configuration of TCP/IP in Windows 2000

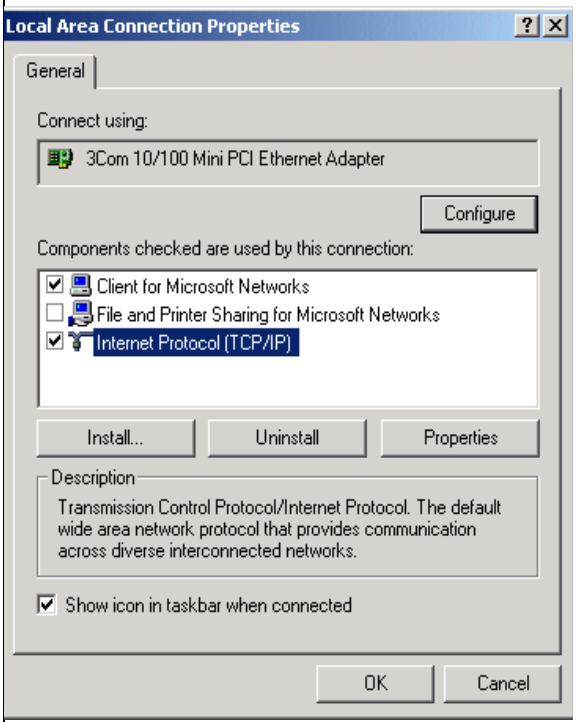
Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

1

- Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.
- Right click on **Local Area Connection** and select **Properties**.

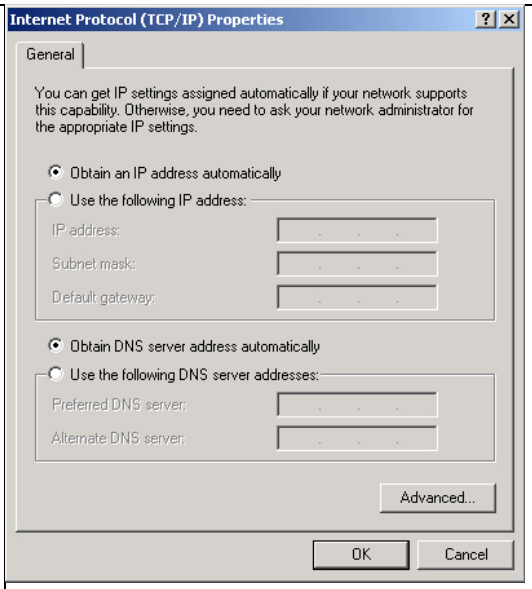
2

- The **Local Area Connection Properties** dialog box appears.
- Verify that you have the correct Ethernet card selected in the **Connect using:** box.
- Verify that at least the following two items are displayed and selected in the box of "Components checked are used by this connection:"
  - Client for Microsoft Networks and
  - Internet Protocol (TCP/IP)
- Click **OK**.



3

- With Internet Protocol (TCP/IP) selected, click on **Properties** to open the Internet Protocol (TCP/IP) Properties dialogue box.
- Verify that
  - **Obtain an IP address automatically** is selected.
  - **Obtain DNS server address automatically** is selected.
- Click **OK** to return to Local Area Connection Properties.

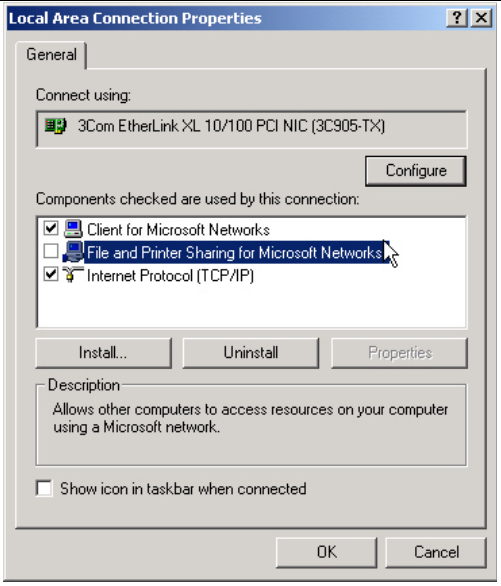


4

- Click **OK** again to complete the configuration process for Windows 2000.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



DHCP Configuration of TCP/IP in Windows NT4

Once you have installed the network card, you need to configure the TCP/IP environment for Windows NT 4.0. Follow this procedure to configure TCP/IP with DHCP in Windows NT 4.0.

1

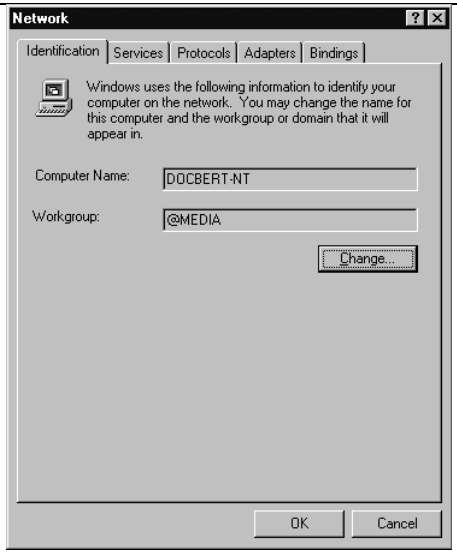
- Choose **Settings** from the Start Menu, and then select **Control Panel**. This will display Control Panel window.

2

- Double-click the **Network** icon in the Control Panel window.

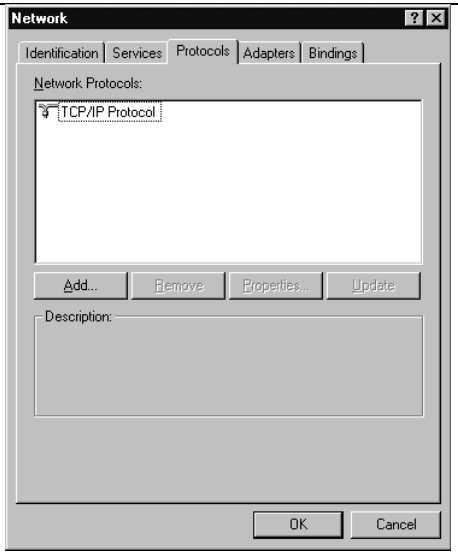
  The Network panel will display.

- Select the **Protocols** tab to continue.



3

- Highlight the **TCP/IP Protocol** in the **Network Protocols** box, and click on the **Properties** button.

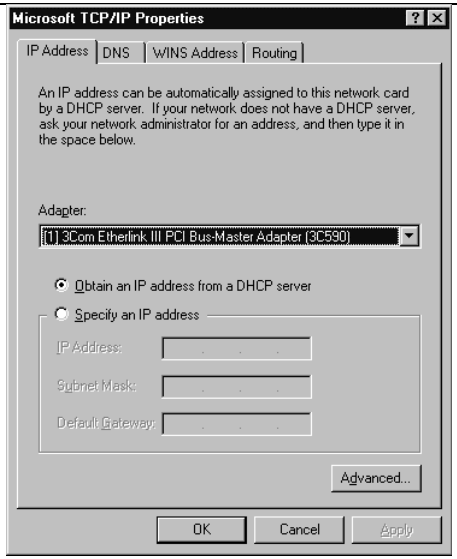


4

- The **TCP/IP Properties** dialog box now displays.
- Click the **IP Address** tab**.**
- Select the radio button marked **Obtain an IP address from a DHCP server.**
- Click **OK**. This completes the configuration of TCP/IP in Windows NT.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.

2. Type **`cmd`** and then click OK.

   A command window opens

3. Type **`ipconfig /all`**

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0

- The default gateway is 192.168.0.1

4. Type **exit**

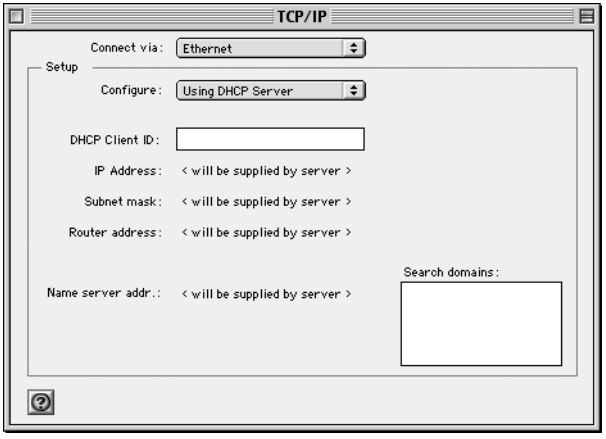
Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you need to configure TCP/IP to use DHCP.

MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens:



2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.

   You can leave the DHCP Client ID box empty.

4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

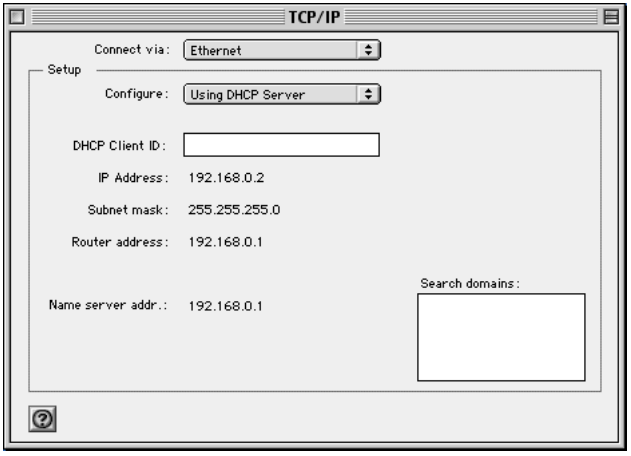
MacOS X

1. From the Apple menu, choose System Preferences, then Network.

2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.



The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

Verifying the Readiness of Your Internet Account

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your router does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your router takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the router's Internet port is connected to the broadband modem, the router appears to be a single PC to the ISP. The router then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the router to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you need to enter your login name and password in the router's configuration menus. After your network and router are configured, the router will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

  For example, your account's full server names may look like this:

  `mail.xxx.yyy.com`

  In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your router automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the router. These procedures are described next.

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the DG834 ADSL router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the router for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components.
3. Select TCP/IP, and then click Properties.

   The TCP/IP Properties dialog box opens.
4. Select the IP Address tab.

   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".
5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

   If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

   You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the DG834 ADSL router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the router for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the "Configure" setting to "Using DHCP Server".

7. Close the TCP/IP Control Panel.

Restarting the Network

Once you have set up your computers to work with the router, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your DG834 ADSL router, you are ready to access and configure the router.

Appendix D
Virtual Private Networking

There have been many improvements in the Internet including Quality of Service, network performance, and inexpensive technologies, such as DSL. But one of the most important advances has been in Virtual Private Networking (VPN) Internet Protocol security (IPSec). IPSec is one of the most complete, secure, and commercially available, standards-based protocols developed for transporting data.

What is a VPN?

A VPN is a shared network where private data is segmented from other traffic so that only the intended recipient has access. The term VPN was originally used to describe a secure connection over the Internet. Today, however, VPN is also used to describe private networks, such as Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS).

A key aspect of data security is that the data flowing across the network is protected by encryption technologies. Private networks lack data security, which allows data attackers to tap directly into the network and read the data. IPSec-based VPNs use encryption to provide data security, which increases the network's resistance to data tampering or theft.

IPSec-based VPNs can be created over any type of IP network, including the Internet, Frame Relay, ATM, and MPLS, but only the Internet is ubiquitous and inexpensive.

VPNs are traditionally used for:

- **Intranets:** Intranets connect an organization's locations. These locations range from the headquarters offices, to branch offices, to a remote employee's home. Often this connectivity is used for e-mail and for sharing applications and files. While Frame Relay, ATM, and MPLS accomplish these tasks, the shortcomings of each limits connectivity. The cost of connecting home users is also very expensive compared to Internet-access technologies, such as DSL or cable. Because of this, organizations are moving their networks to the Internet, which is inexpensive, and using IPSec to create these networks.

- **Remote Access:** Remote access enables telecommuters and mobile workers to access e-mail and business applications. A dial-up connection to an organization's modem pool is one method of access for remote workers, but is expensive because the organization must pay the associated long distance telephone and service costs. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.
- **Extranets**: Extranets are secure connections between two or more organizations. Common uses for extranets include supply-chain management, development partnerships, and subscription services. These undertakings can be difficult using legacy network technologies due to connection costs, time delays, and access availability. IPSec-based VPNs are ideal for extranet connections. IPSec-capable devices can be quickly and inexpensively installed on existing Internet connections.

What Is IPSec and How Does It Work?

IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in while in transit.

IPSec Security Features

IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:

- **Authentication:** Verifies that the packet received is actually from the claimed sender.
- **Integrity:** Ensures that the contents of the packet did not change in transit.
- **Confidentiality:** Conceals the message content through encryption.

IPSec Components

IPSec contains the following elements:

- **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity.
- **Authentication Header (AH)**: Provides authentication and integrity.
- **Internet Key Exchange (IKE)**: Provides key management and Security Association (SA) management.

Encapsulating Security Payload (ESP)

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms IPSec uses produce a unique and unforgeable identifier for each packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to determine if a packet has been tampered with. Furthermore, packets that are not authenticated are discarded and not delivered to the intended receiver.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/ decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

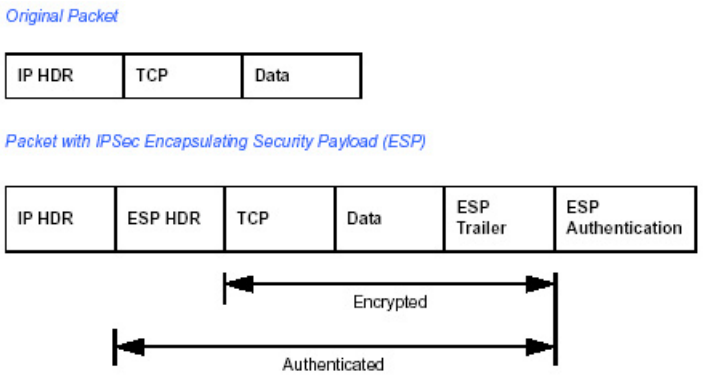


Figure D-1: Original packet and packet with IPSec Encapsulated Security Payload

The ESP header is inserted into the packet between the IP header and any subsequent packet contents. However, because ESP encrypts the data, the payload is changed. ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

Authentication Header (AH)

AH provides authentication and integrity, which protect against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched.

Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.

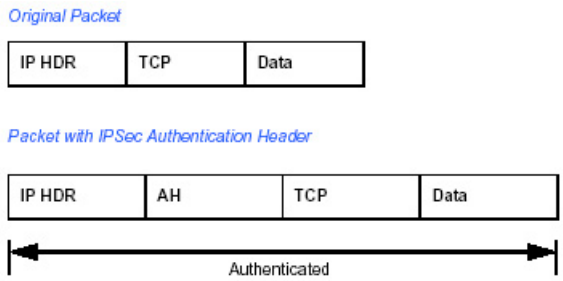


Figure D-2: Original packet and packet with IPSec Authentication Header

IKE Security Association

IPSec introduces the concept of the Security Association (SA). An SA is a logical connection between two devices transferring data. An SA provides data protection for unidirectional traffic by using the defined IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

The SAs allow an enterprise to control exactly what resources may communicate securely, according to security policy. To do this an enterprise can set up multiple SAs to enable multiple secure VPNs, as well as define SAs within the VPN to support different departments and business partners.

Mode

SAs operate using modes. A mode is the method in which the IPSec protocol is applied to the packet. IPSec can be used in tunnel mode or transport mode. Typically, the tunnel mode is used for gateway-to-gateway IPSec tunnel protection, while transport mode is used for host-to-host IPSec tunnel protection. A gateway is a device that monitors and manages incoming and outgoing network traffic and routes the traffic accordingly. A host is a device that sends and receives network traffic.

- **Transport Mode:** The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload. Transport mode does not shield the information in the IP header; therefore, an attacker can learn where the packet is coming from and where it is going to. The previous packet diagrams show a packet in transport mode.
- **Tunnel Mode:** The tunnel mode IPSec implementation encapsulates the entire IP packet. The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Note: AH and ESP can be used in both transport mode or tunnel mode.

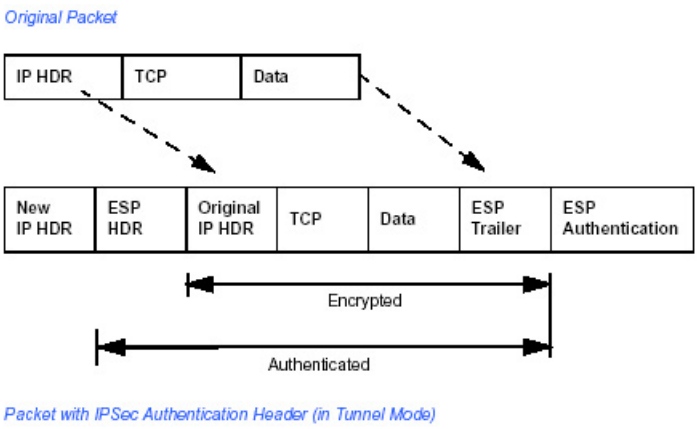


Figure D-3: Original packet and packet with IPSec ESP in Tunnel mode

Key Management

IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it.

IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

Understand the Process Before You Begin

This document provides case studies on how to configure secure IPSec VPN tunnels. This document assumes the reader has a working knowledge of NETGEAR management systems.

NETGEAR is a member of the VPN Consortium, a group formed to facilitate IPSec VPN vendor interoperability. The VPN Consortium has developed specific scenarios to aid system administrators in the often confusing process of connecting two different vendor implementations of the IPSec standard. The case studies in this TechNote follow the addressing and configuration mechanics defined by the VPN Consortium. Additional information regarding inter-vendor interoperability may be found at *http://www.vpnc.org/interop.html*.

It is a good idea to gather all the necessary information required to establish a VPN before you begin the configuration process. You should understand 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. Try to understand any incompatibilities before you begin, so that you minimize any potential complications which may arise from normal firewall or WAN processes.

If you are not a full-time system administrator, it is a good idea to familiarize yourself with the mechanics of a VPN. The brief description in this TechNote will help. Other good sources include:

- The NETGEAR VPN Tutorial – http://www.netgear.com/planetvpn/pvpn_2.html
- The VPN Consortium – http://www.vpnc.org/
- The VPN bibliography in “Additional Reading“ on page D-11.

VPN Process Overview

Even though IPSec is standards-based, each vendor has its own set of terms and procedures for implementing the standard. Because of these differences, it may be a good idea to review some of the terms and the generic processes for connecting two gateways before diving into to the specifics.

Network Interfaces and Addresses

The VPN gateway is aptly named because it functions as a “gatekeeper” for each of the computers connected on the Local Area Network behind it.

In most cases, each Gateway will have a “public” facing address (WAN side) and a “private” facing address (LAN side). These addresses are referred to as the “network interface” in documentation regarding the construction of VPN communication.

Interface Addressing

This Appendix uses example addresses provided the VPN Consortium. It is important to understand that you will be using addresses specific to the devices that you are attempting to connect via IPSec VPN.

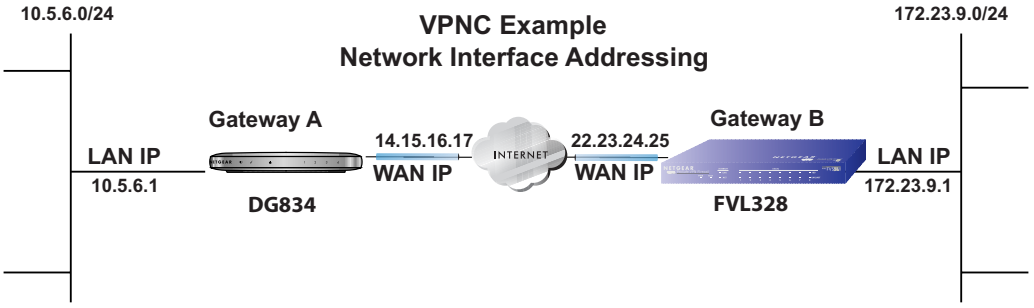


Figure D-4: VPNC Example Network Interface Addressing

It is also important to make sure the addresses do not overlap or conflict. That is, each set of addresses should be separate and distinct.

Table D-1. WAN (Internet/Public) and LAN (Internal/Private) Addressing

Gateway	LAN or WAN	VPNC Example Address
Gateway A	LAN (Private)	10.5.6.1
Gateway A	WAN (Public)	14.15.16.17
Gateway B	LAN (Private)	22.23.24.25
Gateway B	WAN (Public)	172.23.9.1

It will also be important to know the subnet mask of both gateway LAN Connections. Use the worksheet in Table 7-1 on page 7-4 to gather the necessary address and subnet mask information to aid in the configuration and troubleshooting process.

Table D-2. Subnet Addressing

Gateway	LAN or WAN	Interface Name	Example Subnet Mask
Gateway A	LAN (Private)	Subnet Mask A	255.255.255.0
Gateway B	LAN (Private)	Subnet Mask B	255.255.255.0

Firewalls

It is important to understand that many gateways are also firewalls. VPN tunnels cannot function properly if firewall settings disallow all incoming traffic. Please refer to the firewall instructions for both gateways to understand how to open specific protocols, ports, and addresses that you intend to allow.

Setting Up a VPN Tunnel Between Gateways

A SA, frequently called a tunnel, is the set of information that allows two entities (networks, PCs, routers, firewalls, gateways) to “trust each other” and communicate securely as they pass information over the Internet.

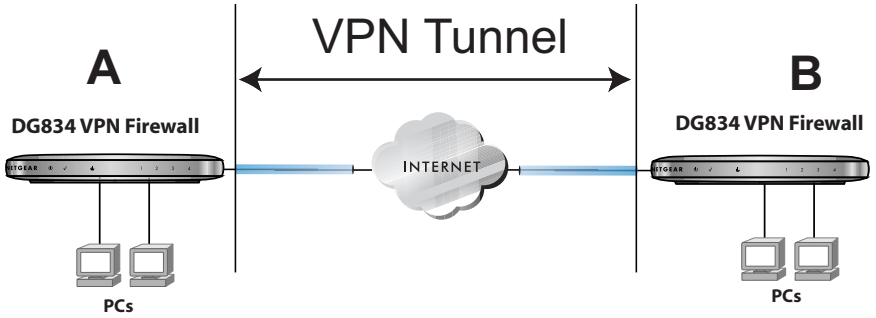


Figure D-5: VPN Tunnel SA

The SA contains all the information necessary for gateway A to negotiate a secure and encrypted communication stream with gateway B. This communication is often referred to as a "tunnel." The gateways contain this information so that it does not have to be loaded onto every computer connected to the gateways.

Each gateway must negotiate its Security Association with another gateway using the parameters and processes established by IPSec. As illustrated below, the most common method of accomplishing this process is via the Internet Key Exchange (IKE) protocol which automates some of the negotiation procedures. Alternatively, you can configure your gateways using manual key exchange, which involves manually configuring each paramter on both gateways.

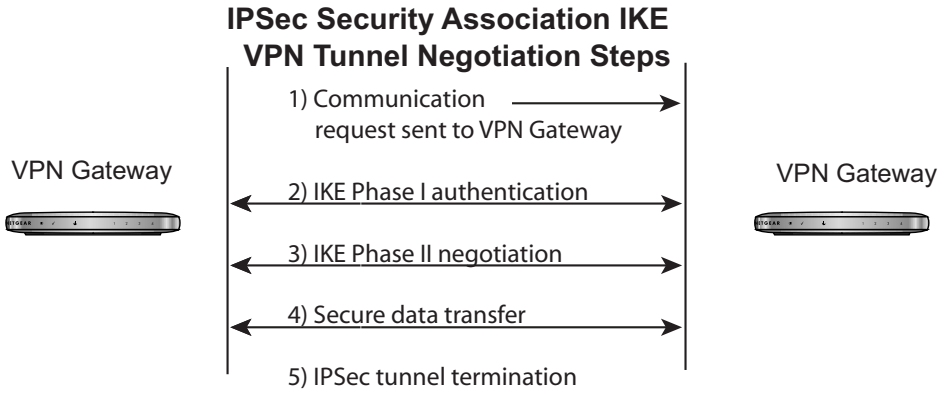


Figure D-6: IPSec SA negotiation

1. **The IPSec software on Host A initiates the IPSec process in an attempt to communicate with Host B.** The two computers then begin the Internet Key Exchange (IKE) process.

2. **IKE Phase I.**
    a. The two parties negotiate the encryption and authentication algorithms to use in the IKE SAs.
    b. The two parties authenticate each other using a predetermined mechanism, such as preshared keys or digital certificates.
    c. A shared master key is generated by the Diffie-Hellman Public key algorithm within the IKE framework for the two parties. The master key is also used in the second phase to derive IPSec keys for the SAs.
3. **IKE Phase II.**
    a. The two parties negotiate the encryption and authentication algorithms to use in the IPSec SAs.
    b. The master key is used to derive the IPSec keys for the SAs. Once the SA keys are created and exchanged, the IPSec SAs are ready to protect user data between the two VPN gateways.
4. **Data transfer.** Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. **IPSec tunnel termination.** IPSec SAs terminate through deletion or by timing out.

VPNC IKE Security Parameters

It is important to remember that both gateways must have the identical parameters set for the process to work correctly. The settings in these TechNote examples follow the examples given for Scenario 1 of the VPN Consortium.

VPNC IKE Phase I Parameters

The IKE Phase 1 parameters used:

- Main mode
- TripleDES
- SHA-1
- MODP group 1
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours)

VPNC IKE Phase II Parameters

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 1
- Perfect forward secrecy for rekeying
- SA lifetime of 28800 seconds (one hour)

Testing and Troubleshooting

Once you have completed the VPN configuration steps you can use PCs, located behind each of the gateways, to ping various addresses on the LAN-side of the other gateway.

You can troubleshoot connections using the VPN status and log details on the Netgear gateway to determine if IKE negotiation is working. Common problems encountered in setting up VPNs include:

- Parameters may be configured differently on Gateway A vs. Gateway B.
- Two LANs set up with similar or overlapping addressing schemes.
- So many required configuration parameters mean errors such as mistyped information or mismatched parameter selections on either side are more likely to happen.

Additional Reading

- *Building and Managing Virtual Private Networks*, Dave Kosiur, Wiley & Sons; ISBN: 0471295264
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick and Steven M. Bellovin, Addison-Wesley; ISBN: 0201633574
- *VPNs A Beginners Guide*, John Mains, McGraw Hill; ISBN: 0072191813
- [FF98] Floyd, S., and Fall, K., Promoting the Use of End-to-End Congestion Control in the Internet. IEEE/ACM Transactions on Networking, August 1999.

Relevant RFCs listed numerically:

- [RFC 791] *Internet Protocol DARPA Internet Program Protocol Specification*, Information Sciences Institute, USC, September 1981.
- [RFC 1058] *Routing Information Protocol*, C Hedrick, Rutgers University, June 1988.
- [RFC 1483] *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, Juha Heinanen, Telecom Finland, July 1993.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.
- [RFC 2407] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.
- [RFC 2474] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.
- [RFC 2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, An Architecture for Differentiated Services, December 1998.
- [RFC 2481] K. Ramakrishnan, S. Floyd, A Proposal to Add Explicit Congestion Notification (ECN) to IP, January 1999.
- [RFC 2408] D. Maughan, M. Schertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol (ISAKMP).
- [RFC 2409] D. Harkins, D.Carrel, Internet Key Exchange (IKE) protocol.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol.

Appendix E
NETGEAR VPN Configuration

DG834 to FVL328

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

Configuration Profile

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

Table E-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)
Date Tested:		June 2004
Model/Firmware Tested:		
	NETGEAR-Gateway A	DG834 firmware version V2.10.17
	NETGEAR-Gateway B	FVL328 with firmware version V2.0_07
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

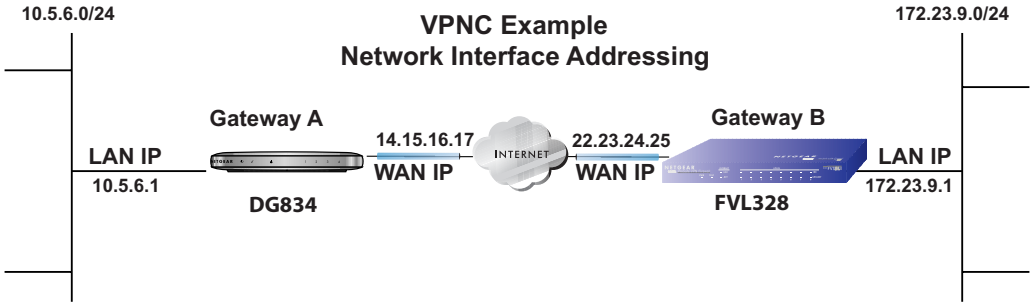


Figure E-1: Addressing and Subnet Used for Examples

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

Step-By-Step Configuration

1. Configure the DG834 as in the Gateway-to-Gateway procedures using the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-20), being certain to use appropriate network addresses for the environment.

   The LAN Addresses used in this example are as follows.

   - DG834
     WAN IP = 14.15.16.17
     LAN IP = 10.5.6.1
     LAN Subnet Mask = 255.255.255.0
   - FVL328
     WAN IP = 22.23.24.25
     LAN IP = 172.23.9.1
     LAN Subnet Mask = 255.255.255.0

   a. In Step 1, enter **toFVL328** for the Connection Name.

   b. In Step 2, enter **22.23.24.25** for the remote WAN's IP address.

   a. In Step 3, enter the following:

   - IP Address = **172.23.9.1**
   - Subnet Mask = **255.255.255.0**

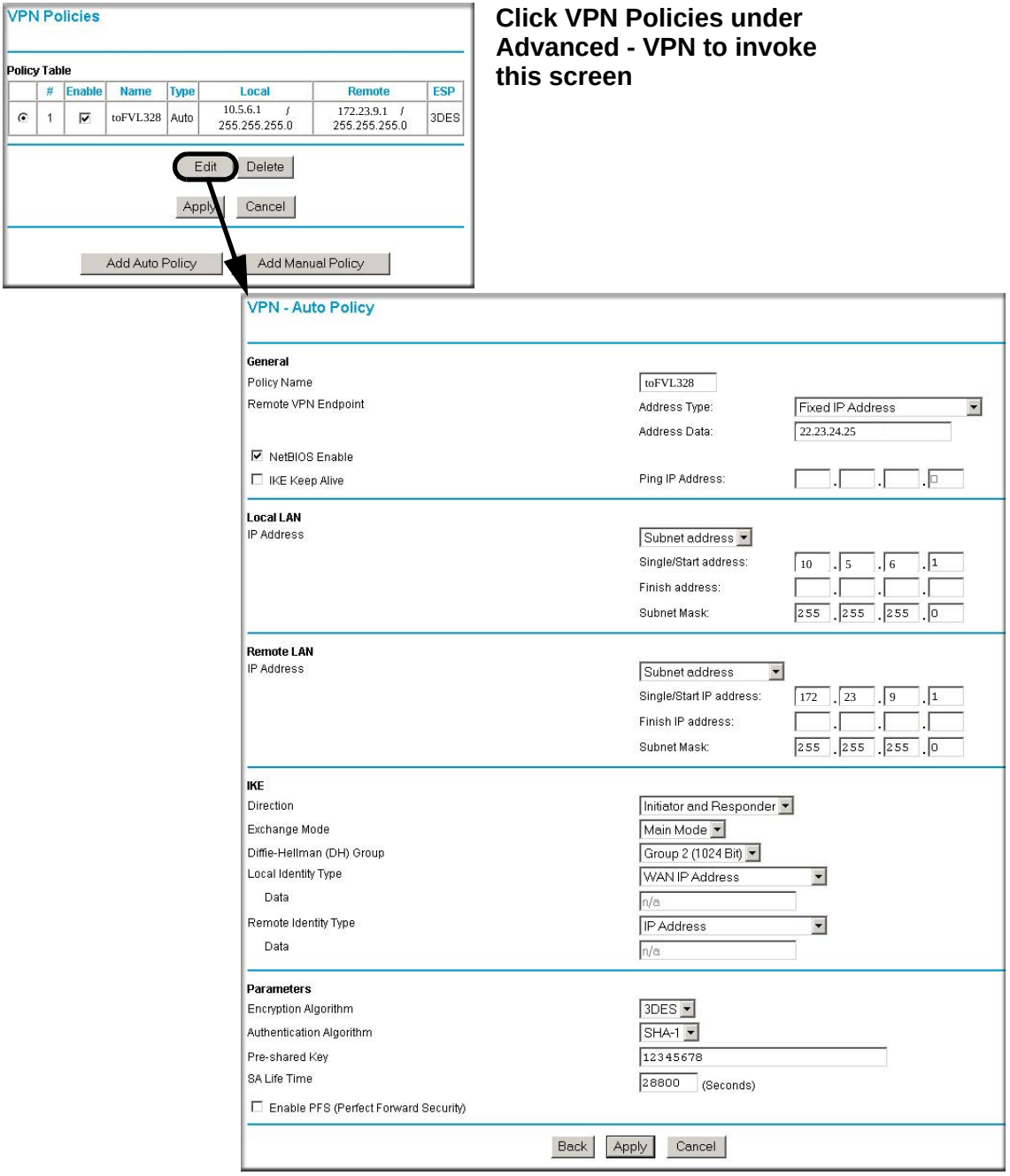


Figure E-2: Viewing and editing the VPN parameters of the DG834 at gateway A

2. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-20), being certain to use appropriate network addresses for the environment.

   a. In Step 1, enter **toDG834** for the Connection Name

   b. In Step 2, enter **14.15.16.17** for the remote WAN's IP address

   c. In Step 3, enter the following:

      - IP Address = **10.5.6.1**
      - Subnet Mask = **255.255.255.0**

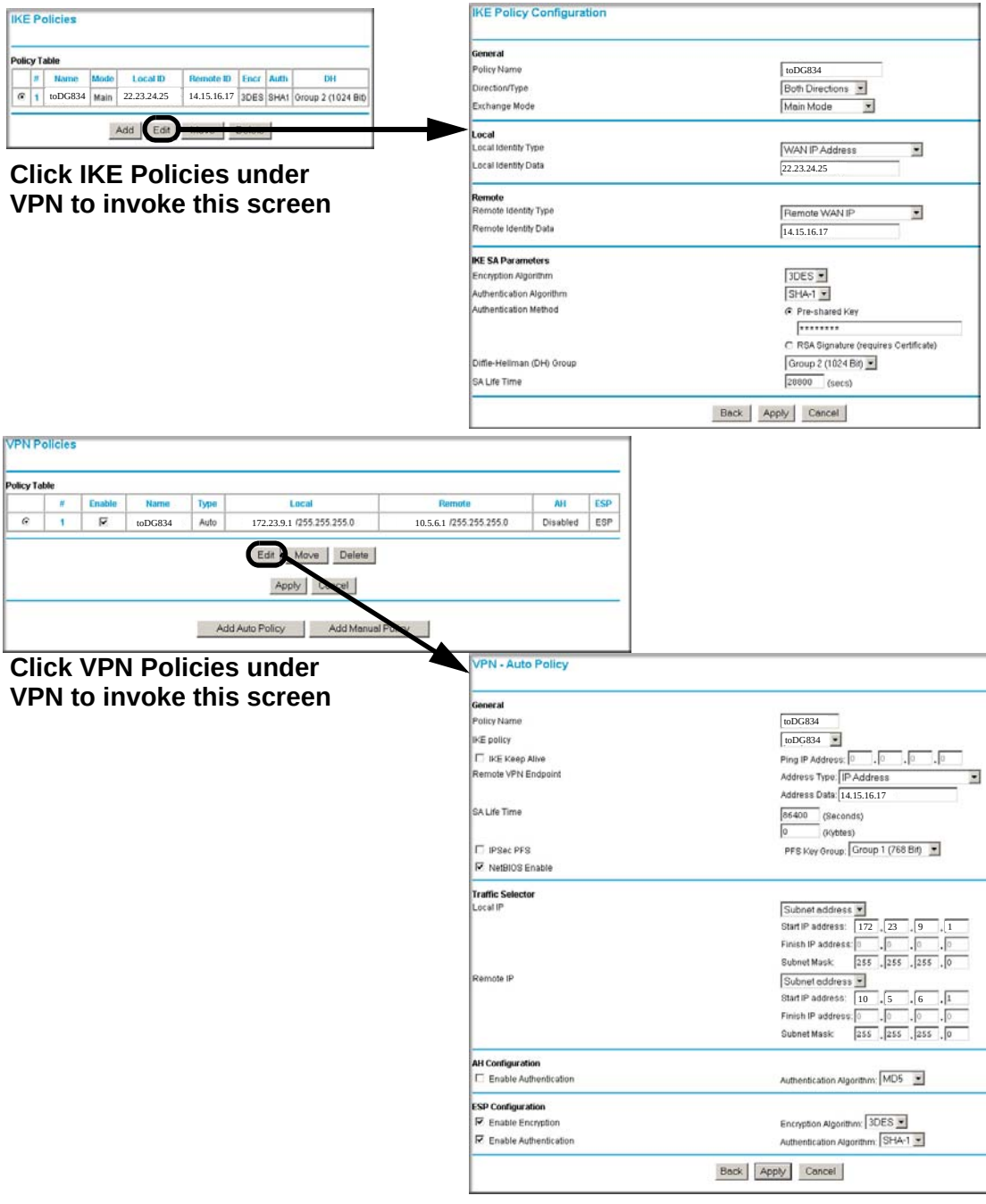


Figure E-3: Viewing and editing the VPN parameters of the FVL328 at gateway B

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

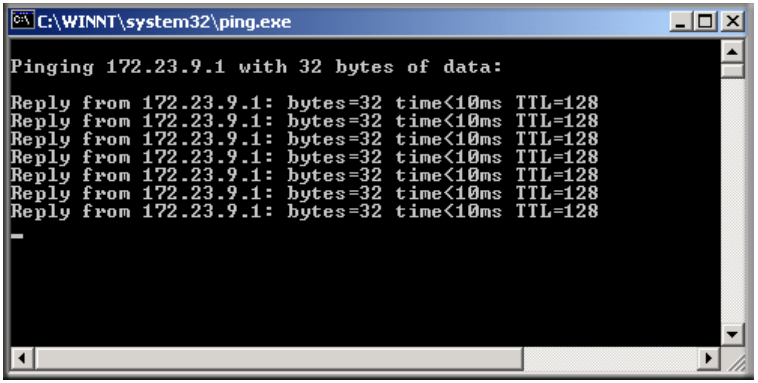


Figure E-4: ping 172.23.9.1

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

DG834 with FQDN to FVL328

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

Configuration Profile

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

Table E-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)
Date Tested:		June 2004
Model/Firmware Tested:		
	NETGEAR-Gateway A	DG834 firmware version V2.10.17
	NETGEAR-Gateway B	FVL328 with firmware version V2.0_07
IP Addressing:		
	NETGEAR-Gateway A	Fully Qualified Domain Name (FQDN)
	NETGEAR-Gateway B	FDQN

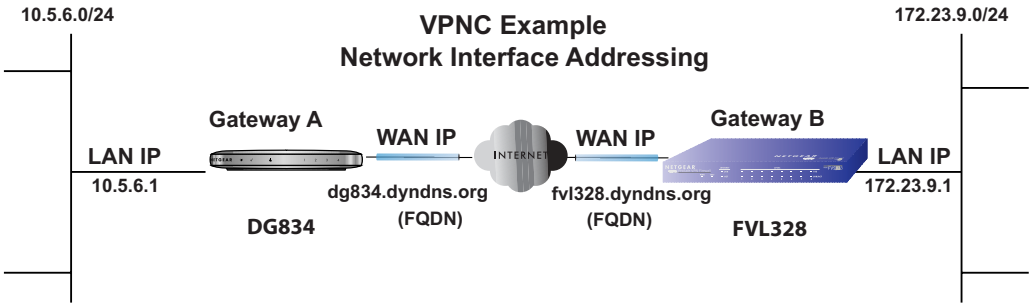


Figure E-5: Addressing and Subnet Used for Examples

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

The Use of a Fully Qualified Domain Name (FQDN)

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

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

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

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

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

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

Step-By-Step Configuration

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

   Out of the box, the DG834 is set for its default LAN address of *http://192.168.0.1* with its default user name of **admin** and default password of **password**. For this example we will assume you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.
2. Click on the Dynamic DNS link on the left side of the Settings management GUI. This will take you to the Dynamic DNS Menu.

3. On the DG834, configure the Dynamic DNS settings.

   a. Browse to the Dynamic DNS Setup Screen (see Figure E-6) in the Advanced menu.

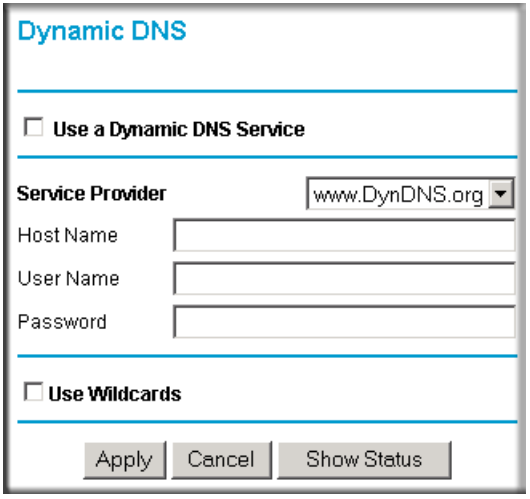


Figure E-6: Dynamic DNS Setup Screen

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

      - Check the box **Use a Dynamic DNS Service**.
      - Host Name = dg834.dyndns.org
      - User Name = <user's account username>
      - Password = <user's account password>

   c. Click **Show Status**. The resulting screen should show Update OK: good (see Figure E-7).

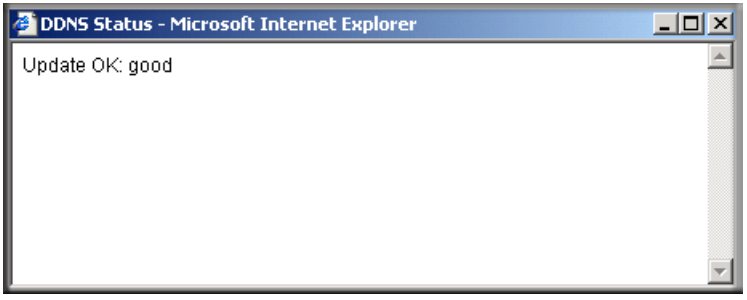


Figure E-7: Status Screen

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

   a. Browse to the Dynamic DNS Setup Screen (see Figure E-8) in the Advanced menu.

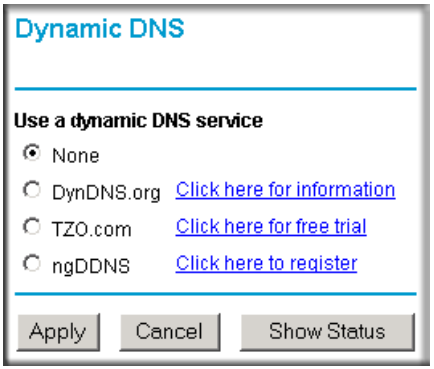


Figure E-8: Dynamic DNS Setup Screen

   b. Select the DynDNS.org radio button (see Figure E-8), configure with appropriate account and hostname settings (see Figure E-9), and then click **Apply**.

      - Host and Domain Name = fvl328.dyndns.org
      - User Name = <user's account username>
      - Password = <user's account password>

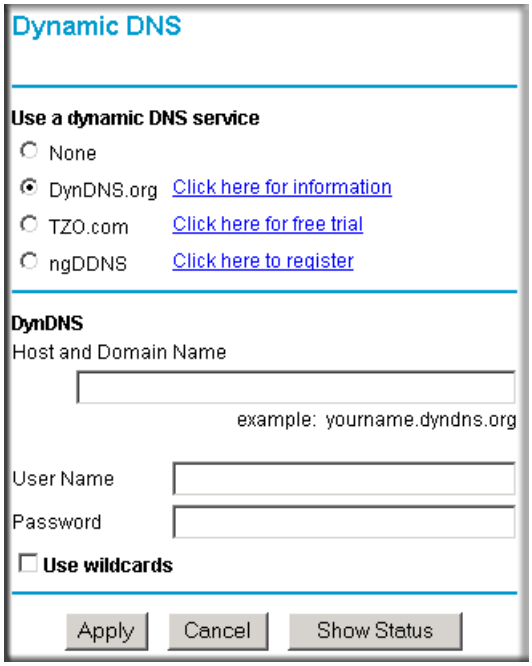


Figure E-9: Dynamic DNS Setup Screen

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

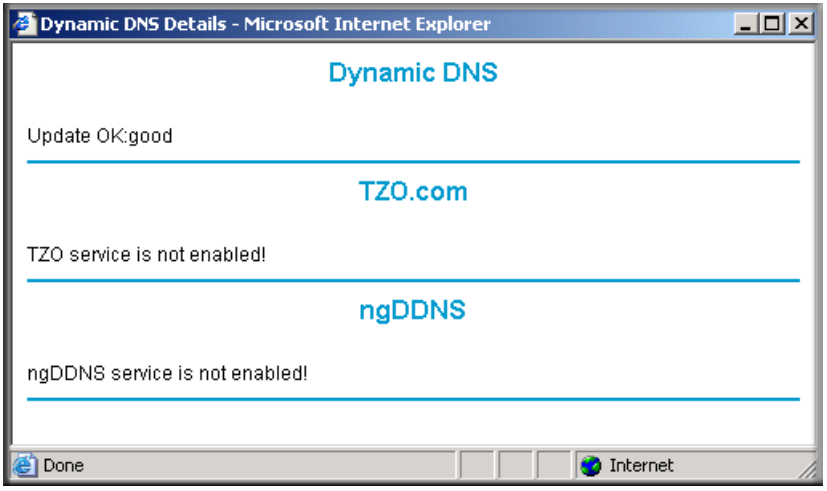


Figure E-10: Status Screen

5. Configure the DG834 as in the Gateway-to-Gateway procedures using the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-20), being certain to use appropriate network addresses for the environment.

   The LAN Addresses used in this example are as follows.

   - DG834
     LAN IP = 10.5.6.1
     LAN Subnet Mask = 255.255.255.0
   - FVL328
     LAN IP = 172.23.9.1
     LAN Subnet Mask = 255.255.255.0

   a. In Step 1, enter **toFVL328** for the Connection Name.

   b. In Step 2, enter **fvl328.dyndns.org** for the remote WAN's IP address.

   a. In Step 3, enter the following:

   - IP Address = **172.23.9.1**
   - Subnet Mask = **255.255.255.0**

6. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 7-20), being certain to use appropriate network addresses for the environment.
   a. In Step 1, enter **toDG834** for the Connection Name.
   b. In Step 2, enter **dg834.dyndns.org** for the remote WAN's IP address.
   c. In Step 3, enter the following:
      - IP Address = **10.5.6.1**
      - Subnet Mask = **255.255.255.0**
7. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834.
   a. Open the command prompt (Start -> Run -> cmd)
   b. ping 172.23.9.1

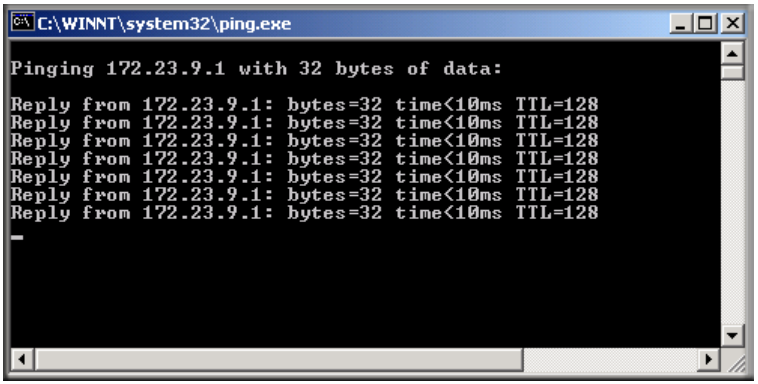


Figure E-11: ping 172.23.9.1

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

Configuration Summary (Telecommuter Example)

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

Table E-1. Configuration summary (telecommuter example)

VPN Consortium Scenario:		Scenario 1
Type of VPN:		PC/client-to-gateway, with client behind NAT router
Security Scheme:		IKE with Preshared Secret/Key (not Certificate-based)
Date Tested:		May 2005
Model/Firmware Tested:		
	Gateway	DG834G firmware version v2.10.20
	Client	NETGEAR ProSafe VPN Client v10.5.1 (build 8)
IP Addressing:		
	Gateway	Fully Qualified Domain Name (FQDN)
	Client	Dynamic

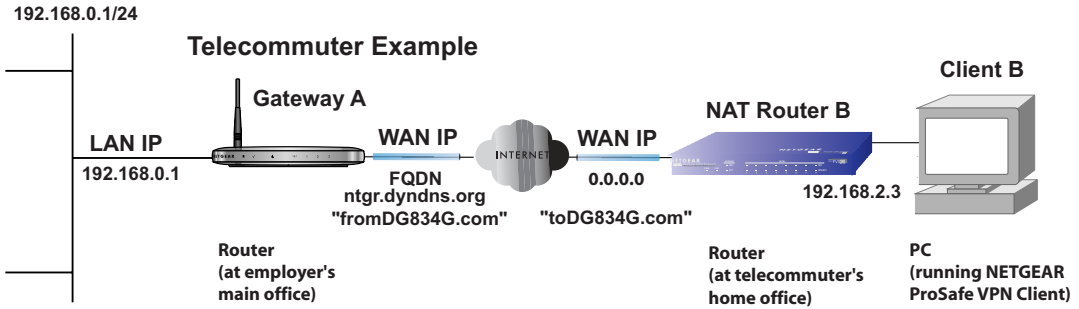


Figure E-12: Addressing and subnet used for telecommuter example

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

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

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

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

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

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

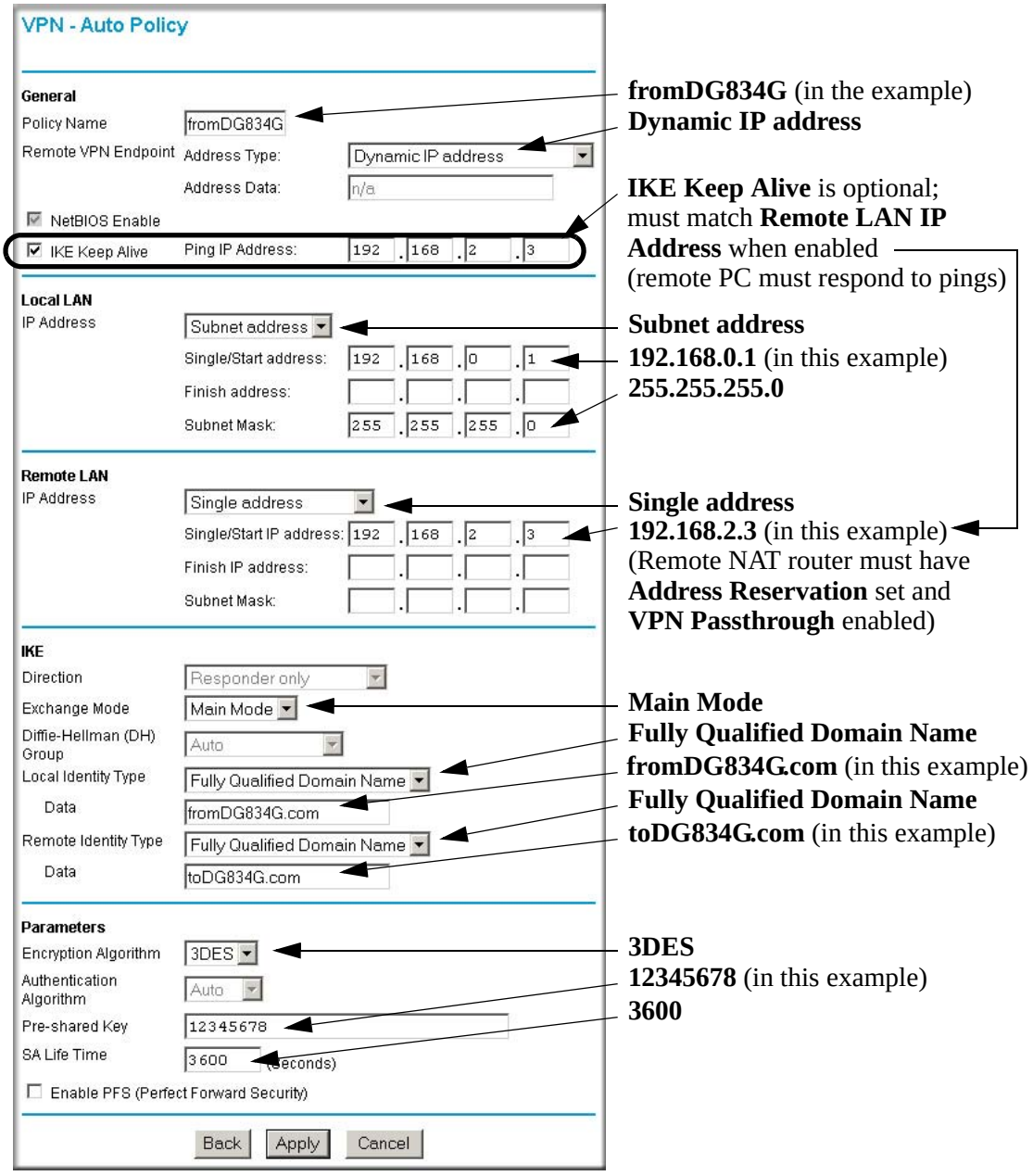


Figure E-13: VPN Auto Policy screen

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

Figure E-14: VPN Policies screen

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

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

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

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

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

1. Install the NETGEA ProSafe VPN Client on the remote PC and reboot.
   a. You may need to insert your Windows CD to complete the installation.

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

c. Install the **IPSec** Component. You may have the option to install either the **VPN Adapter** or the **IPSec Component** or both. The **VPN Adapter** is not necessary.

d. The system should show the **ProSafe** icon ( ) in the system tray after rebooting.

e. Double-click the system tray icon to open the **Security Policy Editor**.

2. Add a new connection.

a. Run the **NETGEAR ProSafe Security Policy Editor** program and create a **VPN Connection**.

b. From the **Edit** menu of the **Security Policy Editor**, click **Add**, then **Connection**. A **New Connection** listing appears in the list of policies. Rename the **New Connection** so that it matches the **Connection Name** you entered in the **VPN Settings** of the DG834 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 E-16) because Connection Names are arbitrary to how the VPN tunnel functions.

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

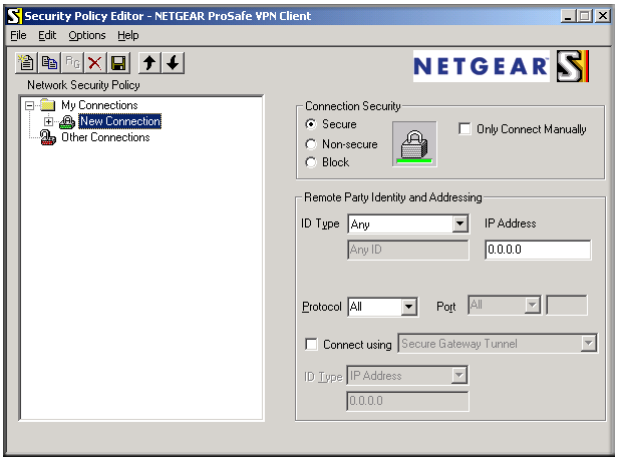


Figure E-15: Security Policy Editor new connection

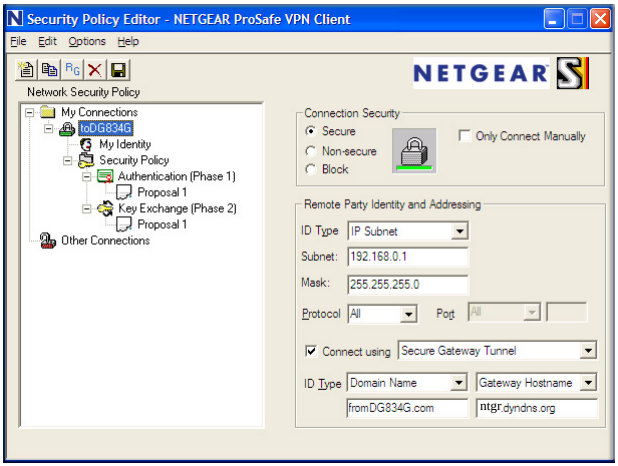


Figure E-16: Security Policy Editor Connection settings

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

d. Select **IP Subnet** in the **ID Type** menu.

e. In this example, type **192.168.0.1** in the Subnet field as the network address of the DG834.

f. Enter **255.255.255.0** in the Mask field as the **LAN Subnet Mask** of the DG834.

g. Select **All** in the **Protocol** menu to allow all traffic through the VPN tunnel.

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

i. Select **Domain Name** in the **ID Type** menu below the check box and enter **fromDG834G.com** (in this example).

j. Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).

k. The resulting Connection Settings are shown in Figure E-16.

3. Configure the **Security Policy** in the DG834 ADSL Firewall Router software.

a. In the **Network Security Policy** list, expand the new connection by double clicking its name or clicking on the “+” symbol. **My Identity** and **Security Policy** subheadings appear below the connection name.

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

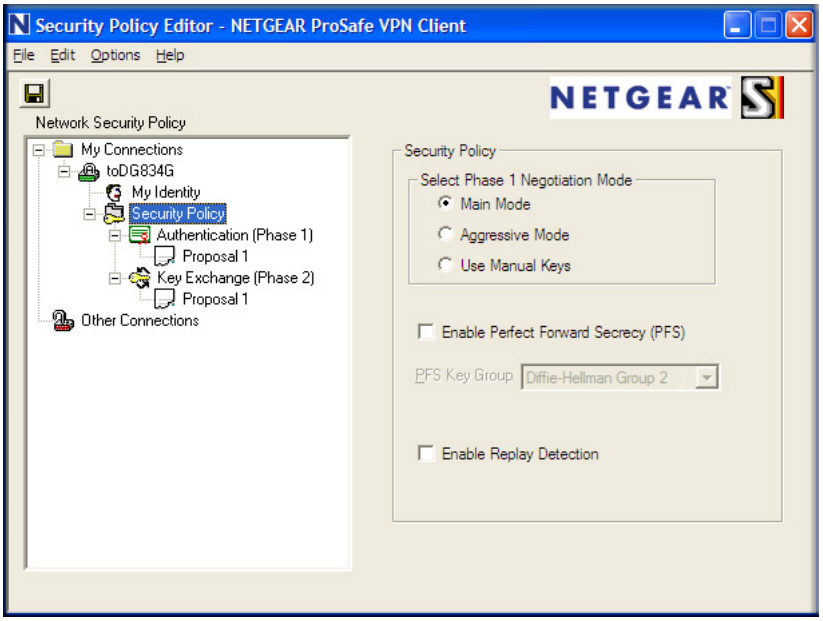


Figure E-17: Security Policy Editor security policy

c. Select the **Main Mode** in the **Select Phase 1 Negotiation Mode** check box.

4. Configure the **VPN Client Identity**.

   In this step, you will provide information about the remote VPN client PC. You will need to provide:

   — The Pre-Shared Key that you configured in the DG834.

   — 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**.

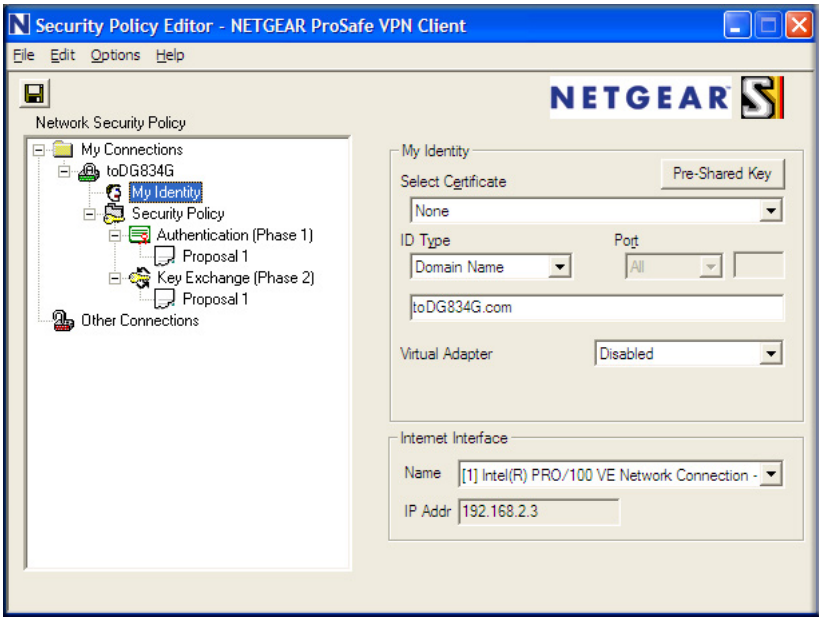


Figure E-18: Security Policy Editor my identity

b. Choose **None** in the **Select Certificate** menu.

c. Select **Domain Name** in the **ID Type** menu and enter **toDG834G.com** (in this example) in the box below it. Choose **Disabled** in the **Virtual Adapter** menu.

d. In the **Internet Interface** box, select **Intel PRO/100VE Network Connection** (in this example, your Ethernet adapter may be different) in the **Name** menu and enter **192.168.2.3** (in this example) in the **IP Addr** box.

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

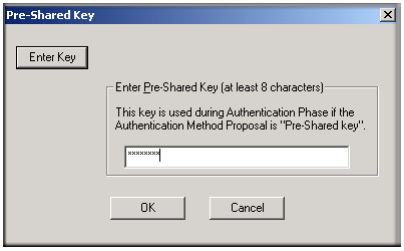


Figure E-19: Security Policy Editor pre-shared key

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

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

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

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

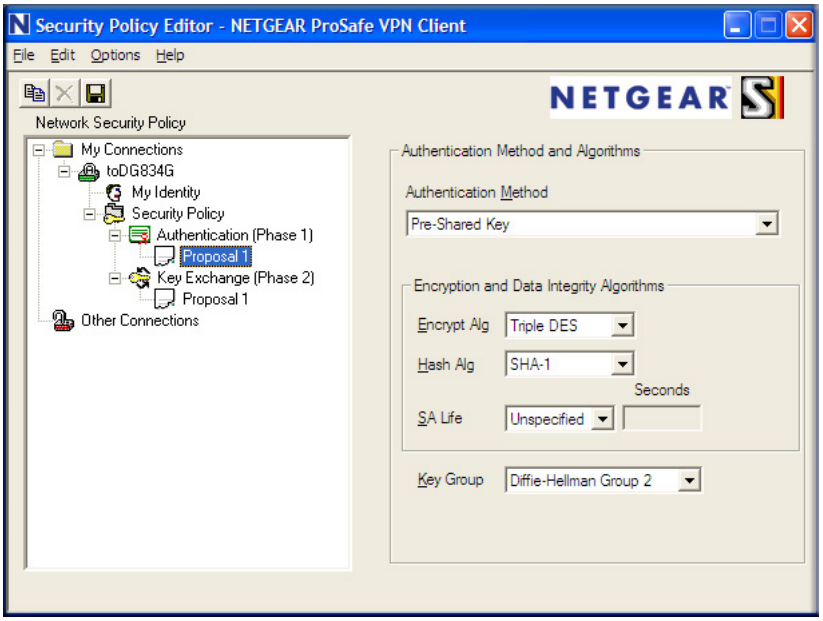


Figure E-20: Security Policy Editor authentication

c. In the **Authentication Method** menu, select **Pre-Shared key**.

d. In the **Encrypt Alg** menu, select the type of encryption. In this example, use **Triple DES**.

e. In the **Hash Alg** menu, select **SHA-1**.

f. In the **SA Life** menu, select **Unspecified**.

g. In the **Key Group** menu, select **Diffie-Hellman Group 2**.

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

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

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

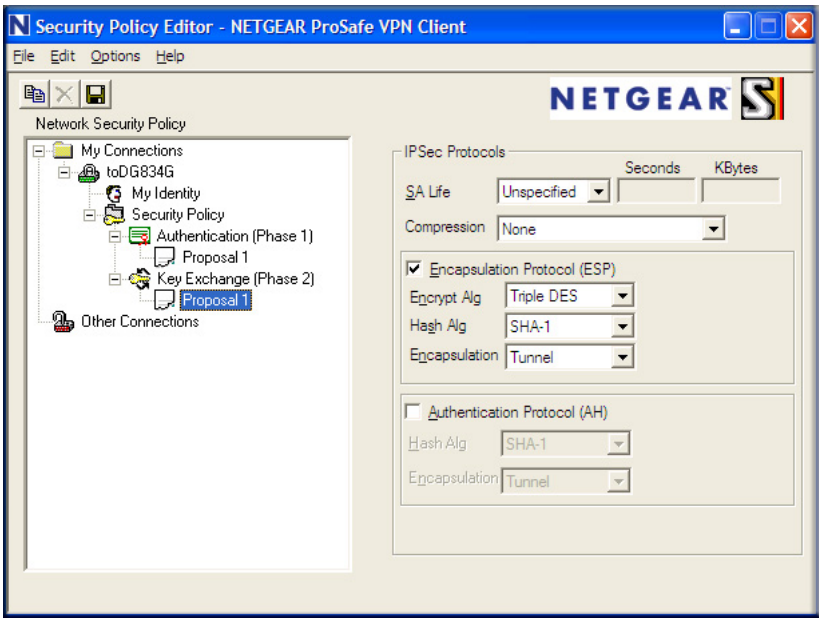


Figure E-21: Security Policy Editor key exchange

b. In the **SA Life** menu, select **Unspecified**.

c. In the **Compression** menu, select **None**.

d. Check the **Encapsulation Protocol (ESP)** checkbox.

e. In the **Encrypt Alg** menu, select the type of encryption. In this example, use **Triple DES**.

f. In the **Hash Alg** menu, select **SHA-1**.

g. In the **Encapsulation** menu, select **Tunnel**.

h. Leave the **Authentication Protocol (AH)** checkbox unchecked.

7. Save the VPN Client settings.

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

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

8. Check the **VPN Connection**.

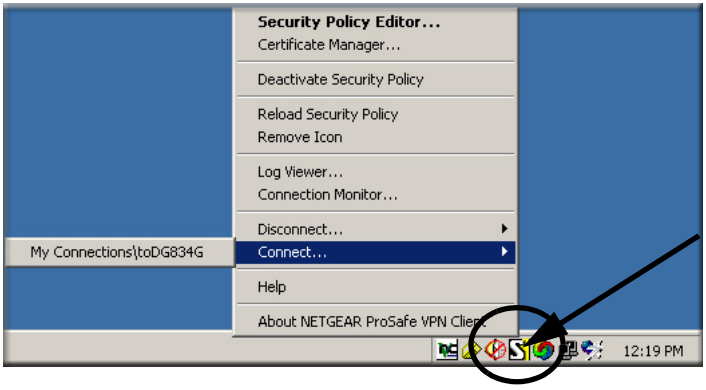
   To check the **VPN Connection**, you can initiate a request from the remote PC to the VPN router's network by using the **Connect** option in the DG834 ADSL router menu bar (see Figure E-22). Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

   a. Right-click the system tray icon to open the popup menu.

   b. Select **Connect** to open the **My Connections** list.

   c. Choose **toDG834G**.

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



Right-mouse-click on the system tray icon to open the popup

Figure E-22: Connecting the PC the DG834G over the VPN tunnel

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

a. Establish an Internet connection from the PC.

b. On the **Windows** taskbar, click the Start **button**, and then click **Run**.

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

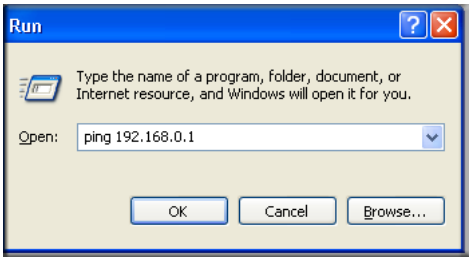


Figure E-23: Running a ping test to the LAN from the PC

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

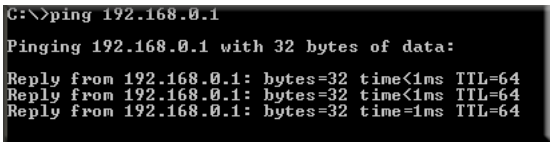


Figure E-24: Ping test results

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

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

Monitoring the VPN Tunnel (Telecommuter Example)

Viewing the PC Client's Connection Monitor and Log Viewer

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

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

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

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

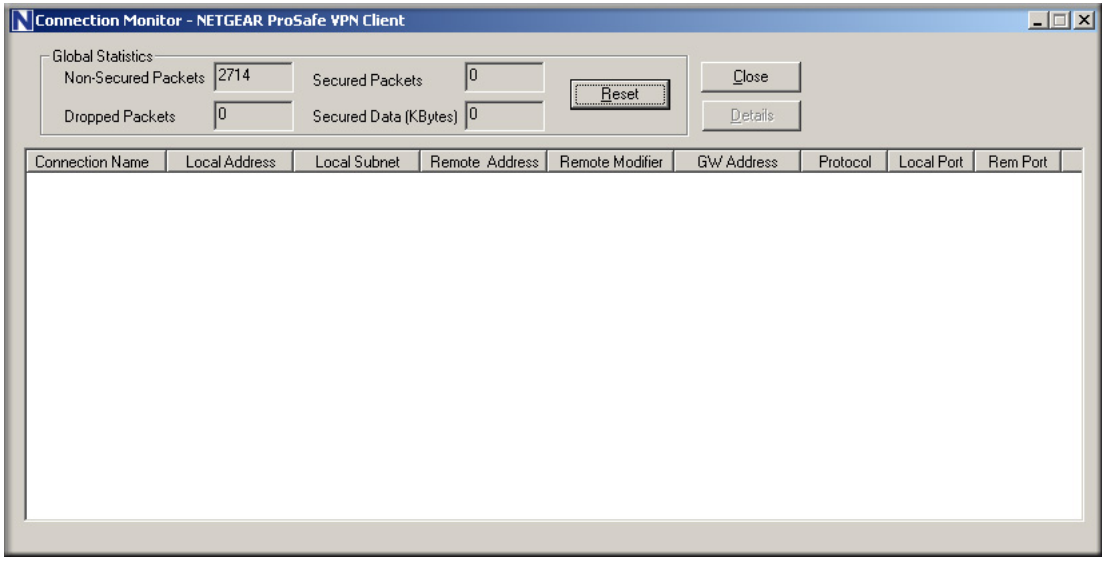


Figure E-25: Connection Monitor screen

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

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

Viewing the VPN Router's VPN Status and Log Information

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

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

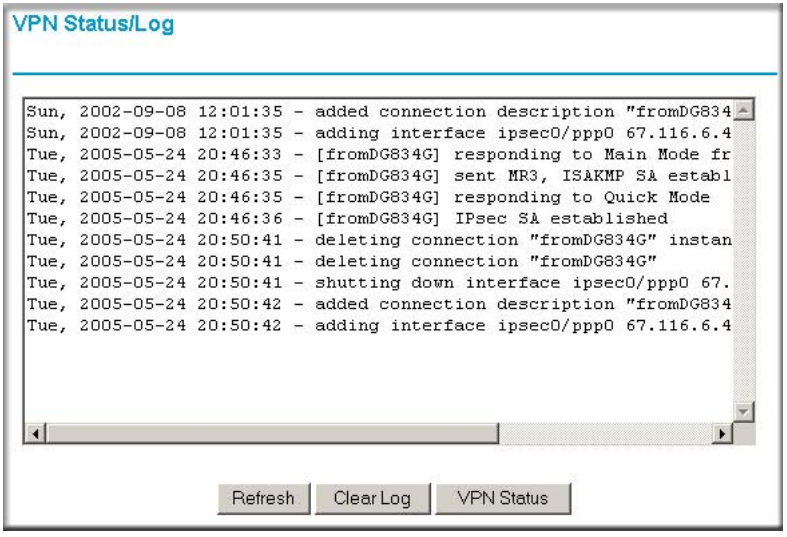
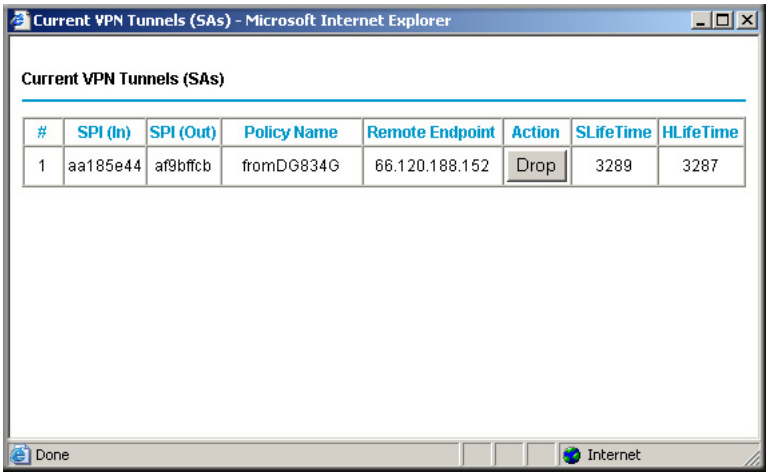


Figure E-26: VPN Status/Log screen

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



Current VPN Tunnels (SAs) screen

Glossary

10BASE-T	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
100BASE-Tx	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
802.11b	IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
802.11g	IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
802.11x	802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management. The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.
Access Control List (ACL)	An ACL is a database that an Operating System uses to track each user's access rights to system objects (such as file directories and/or files).
Ad-hoc Mode	An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required.
ADSL	*See* Asymmetric Digital Subscriber Line
Asymmetric Digital Subscriber Line	A technology for sending data over regular telephone lines. ADSL allows data rates up to 8 Mbps downstream and 640 Kbps upstream.

Cat 5	Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.
Denial of Service attack	DoS. A hacker attack designed to prevent your computer or network from operating or communicating.
DHCP	*See* Dynamic Host Configuration Protocol.
DMZ	Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you have not defined. There are security issues with doing this, so only do this if you are willing to risk open access
DNS	*See* Domain Name Server.
Domain Name	A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, and so on. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.
Domain Name Server	A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
DSLAM	DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.
Dynamic Host Configuration Protocol	DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.
Gateway	A local device, usually a router, that connects hosts on a local network to other networks.
IP	*See* Internet Protocol.

IP Address	A four-byte number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
IPSec	Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.
ISP	Internet service provider.
Internet Protocol	The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
LAN	*See* local area network.
local area network	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.
MAC address	Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.
Mbps	Megabits per second.
MDI/MDIX	In cable wiring, the concept of transmit and receive are from the perspective of the computer, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a computer transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).
MSB	*See* Most Significant Bit or Most Significant Byte.
MTU	*See* Maximum Transmission Unit.
Maximum Transmit Unit	The size in bytes of the largest packet that can be sent or received.
Most Significant Bit or Most Significant Byte	The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.
NAT	*See* Network Address Translation.

Netmask	A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.
Network Address Translation	A technique by which several hosts share a single IP address for access to the Internet.
packet	A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.
PPP	*See* Point-to-Point Protocol.
PPPoA	*See* PPP over ATM
PPPoE	*See* PPP over Ethernet
PPP over ATM	PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
PPP over Ethernet	PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
PPTP	Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.
PSTN	Public Switched Telephone Network.
Point-to-Point Protocol	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
RADIUS	Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system. Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.
RFC	Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at www.ietf.org.
RIP	*See* Routing Information Protocol.

router	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
Routing Information Protocol	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
SSID	A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless computer card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID
subnet mask	*See* netmask.
Universal Plug and Play	UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, video conferencing and other peer-to-peer services.
UTP	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.
VCI	Virtual Channel Identifier. Together with the VPI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.
VPI	Virtual Path Identifier. Together with the VCI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.
WAN	*See* wide area network.
WEP	Wired Equivalent Privacy. WEP is a data encryption protocol for 802.11b wireless networks. All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.
wide area network	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
Wi-Fi	*See* 802.11b. A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11b devices.

Windows Internet Naming Service	WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using Network Neighborhood.
WINS	*See* Windows Internet Naming Service.
WPA	Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.