

## Configuring Dynamic DNS

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

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

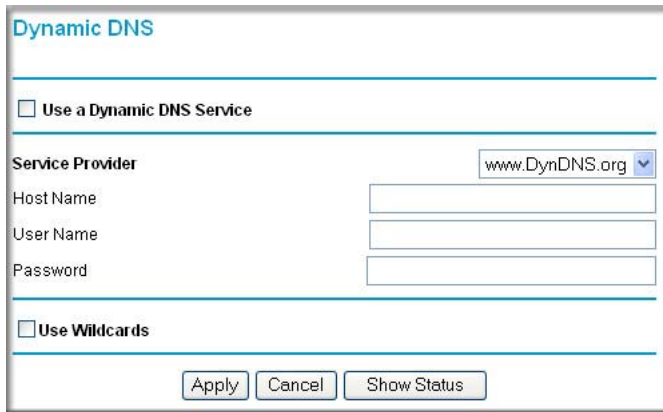
## How to Configure Dynamic DNS



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

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

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



The screenshot shows a web form titled "Dynamic DNS". At the top, there is a checkbox labeled "Use a Dynamic DNS Service". Below this, there is a "Service Provider" dropdown menu with "www.DynDNS.org" selected. Underneath are three text input fields for "Host Name", "User Name", and "Password". At the bottom of the form, there is another checkbox labeled "Use Wildcards". At the very bottom, there are three buttons: "Apply", "Cancel", and "Show Status".

**Figure 7-4**

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

## Using Static Routes

---

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

### Static Route Example

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

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

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

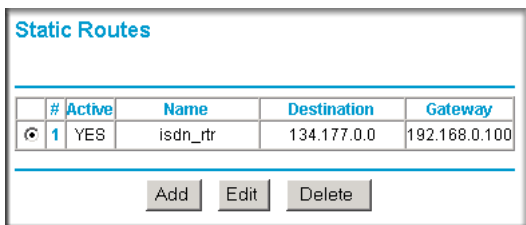
In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like [Figure 7-6](#).

In this example:

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

## How to Configure Static Routes

1. Log in to the router at its default LAN address of `http://192.168.0.1` with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, click **Static Routes** to view the Static Routes menu, shown in [Figure 7-5](#).



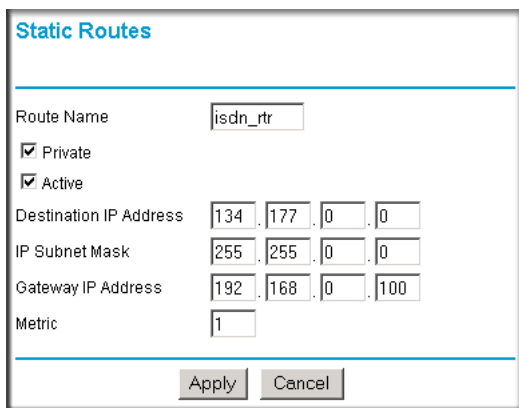
The screenshot shows the 'Static Routes' configuration page. It features a table with the following data:

#	Active	Name	Destination	Gateway
1	YES	isdn_rtr	134.177.0.0	192.168.0.100

Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

**Figure 7-5**

3. To add or edit a Static Route:
  - a. Click the **Edit** button to open the Edit Menu, shown in [Figure 7-6](#).



The screenshot shows the 'Static Routes' Edit Menu. It contains the following fields and options:

- Route Name:
- Private
- Active
- Destination IP Address:  .  .  .
- IP Subnet Mask:  .  .  .
- Gateway IP Address:  .  .  .
- Metric:

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

**Figure 7-6**

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

- d. Select **Active** to make this route effective.
  - e. Type the Destination IP Address of the final destination.
  - f. Type the IP Subnet Mask for this destination.  
If the destination is a single host, type 255.255.255.255.
  - g. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.
  - h. Type a number between 2 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 2.
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 7-7**

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

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

## Wireless Bridging and Repeating

---

The ADSL Modem Wireless Router lets you build large bridged wireless networks by being configured into a Wireless Distribution System (WDS).

Examples of wireless bridged configurations are:

- **Point-to-Point Bridge.** The DG834G v4 communicates with another bridge-mode wireless station. See [“Point-to-Point Bridge Configuration” on page 7-16.](#)
- **Multi-Point Bridge.** The DG834G v4 is the “master” for a group of bridge-mode wireless stations. Then all traffic is sent to this “master,” rather than to other access points. See [“Multi-Point Bridge Configuration” on page 7-17.](#)

- **Repeater with Wireless Client Association.** Sends all traffic to the remote AP. See “[Repeater with Wireless Client Association](#)” on page 7-19.



**Note:** The Wireless Bridging and Repeating feature uses the default Security Profile to send and receive traffic.

These configurations can be set up from the Advanced Access Point Settings page, shown in [Figure 7-1](#) below.



### Advanced Wireless Settings

---

**WDS Mode**

Enable Wireless Bridging and Repeating

**Wireless Point-to-Point Bridge**

Local MAC Address  :  :  :  :  :

Remote MAC Address  :  :  :  :  :

**Wireless Point to Multi-Point Bridge**

Local MAC Address  :  :  :  :  :

Remote MAC Address 1  :  :  :  :  :

Remote MAC Address 2  :  :  :  :  :

Remote MAC Address 3  :  :  :  :  :

Remote MAC Address 4  :  :  :  :  :

**Repeater with Wireless Client Association**

Local MAC Address  :  :  :  :  :

Remote MAC Address 1  :  :  :  :  :

Remote MAC Address 2  :  :  :  :  :

Remote MAC Address 3  :  :  :  :  :

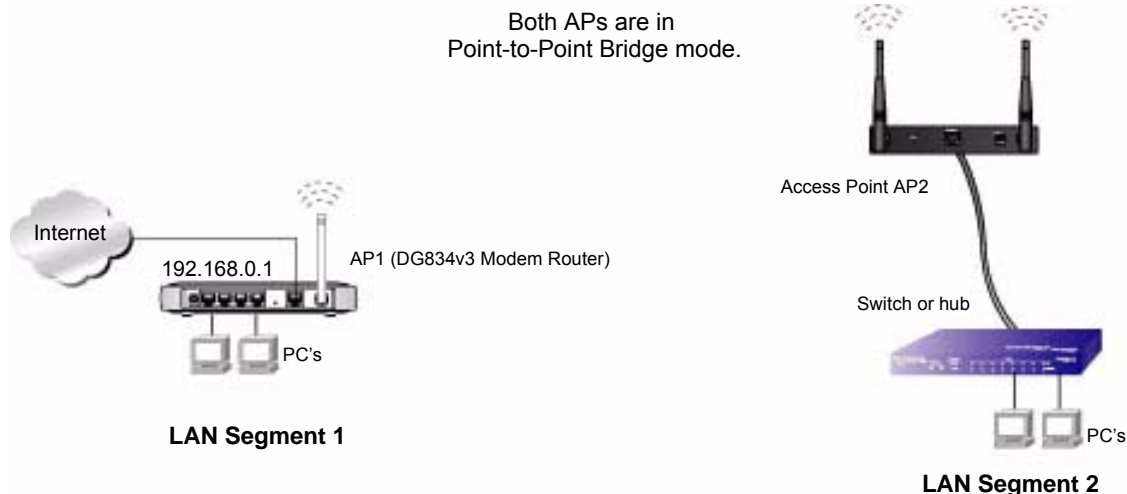
Remote MAC Address 4  :  :  :  :  :

---

**Figure 7-1**

## Point-to-Point Bridge Configuration

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



**Figure 7-2**

The following steps describe how to set up the Point-to-Point Bridge configuration in [Figure 7-2](#).

1. Configure the DG834G v4 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the other access point (AP2) on LAN Segment 2 in Point-to-Point Bridge mode.

The DG834G v4 must have AP2's MAC address in its Remote MAC Address field, and AP2 must have the DG834G v4's MAC address in its Remote MAC Address field.

3. Configure and verify the following for both access points:
  - Both APs must use the same SSID, Channel, authentication mode, if any, and security settings if security is in use.
4. Verify connectivity across LAN Segment 1 and LAN Segment 2.

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



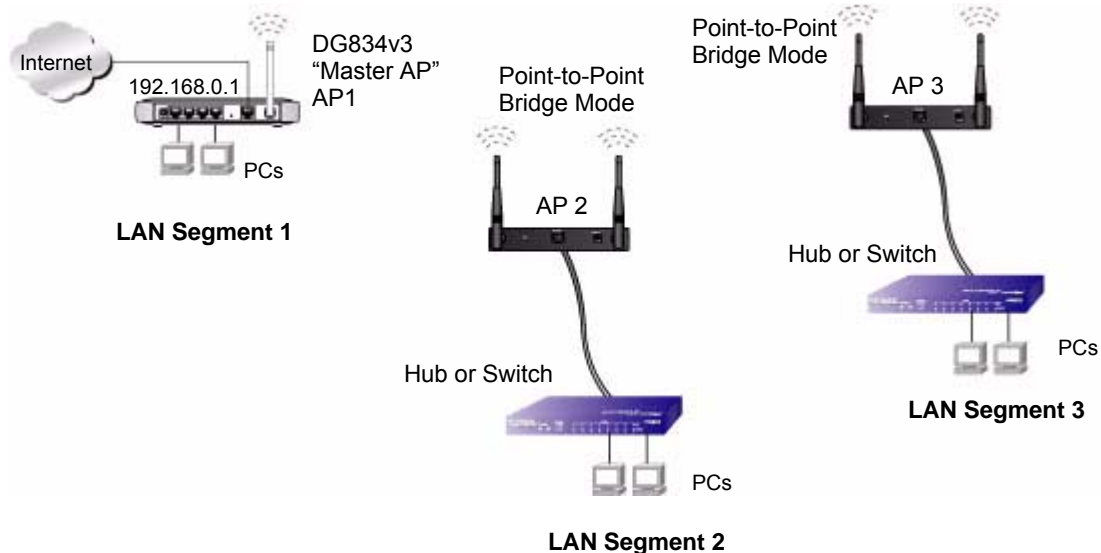
## Multi-Point Bridge Configuration

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

- Entering the MAC addresses of the other access points in the fields provided.
- Setting the other bridge-mode access points to Point-to-Point Bridge mode, using the MAC address of this DG834G v4 as the Remote MAC Address.
- Using wireless security to protect this traffic.

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

Point-to-Multi-Point  
Bridge mode



**Figure 7-3**

The following steps describe how to set up the Multi-Point Bridge configuration shown in [Figure 7-3](#).

1. Configure the Operating Mode of the ADSL Modem Wireless Routers.
  - Because it is in a central location, configure the DG834G v4 (AP 1) on LAN Segment 1 in Point-to-Multi-Point Bridge mode and enter the MAC addresses of AP 2 and AP 3 in the Remote MAC Address 1 and Remote MAC Address 2 fields.

- Configure the access point (AP2) on LAN Segment 2 in Point-to-Point Bridge mode with the Remote MAC Address of the DG834G v4 ADSL Modem Wireless Router.
  - Configure the access point (AP3) on LAN Segment 3 in Point-to-Point Bridge mode with the Remote MAC Address of the DG834G v4 ADSL Modem Wireless Router.
2. Verify the following for all access points:
- The LAN network configuration of the ADSL Modem Wireless Router and other access points are configured to operate in the same LAN network address range as the LAN devices
  - Only one AP, the DG834G v4 in [Figure 7-3](#), is configured in Point-to-Multi-Point Bridge mode; all the others are in Point-to-Point Bridge mode.
  - All APs, including the DG834G v4 ADSL Modem Wireless Router, must be on the same LAN. That is, all the AP LAN IP addresses must be in the same network.
  - If using DHCP, all access points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
  - All APs, including the DG834G v4 ADSL Modem Wireless Router, must use the same SSID, Channel, authentication mode, if any, and encryption in use.
  - All Point-to-Point APs must have the MAC address of AP1 (the DG834G v4 ADSL Modem Wireless Router in the above diagram) in the Remote AP MAC address field.
3. Verify connectivity across the LANs.
- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.



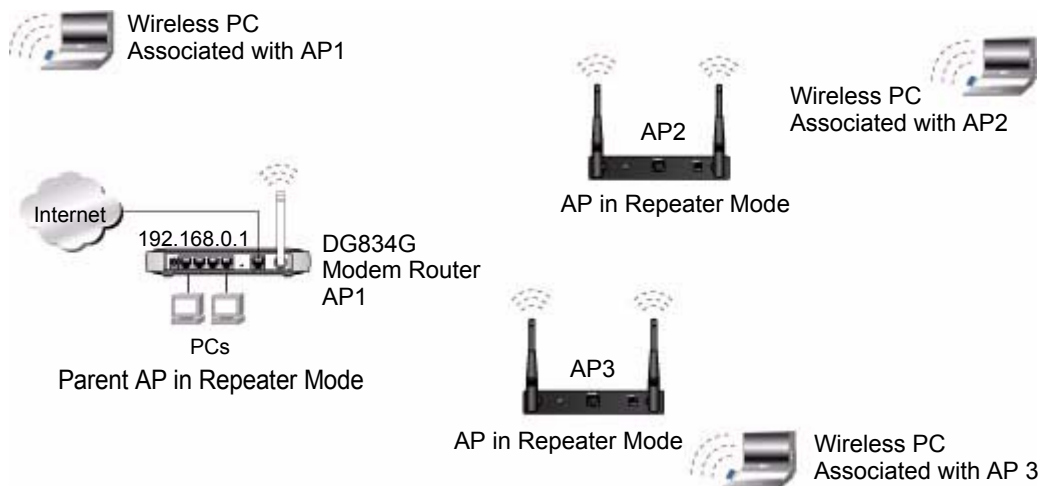
**Note:** Wireless stations will not be able to connect to the ADSL Modem Wireless Router or access points in [Figure 7-3](#). If you require wireless stations to access any LAN segment, you can use additional access points configured in Wireless Access Point mode in any LAN segment.

## Repeater with Wireless Client Association

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

- You *do not* have the option of disabling client associations with this ADSL Modem Wireless Router.
- You cannot configure a sequence of parent/child APs. You are limited to only one parent AP, although if the DG834G v4 is the parent AP it can connect with up to four child APs.

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



**Figure 7-4**

To set up a repeater with wireless client association, follow the steps below:

1. Configure the Operating Mode of the ADSL Modem Wireless Router devices.
  - Configure AP1 (the the DG834G v4 ADSL Modem Wireless Router in the above diagram) on LAN Segment 1 with the MAC address of AP2 and AP3 in the first two Remote MAC Address fields.
  - Configure AP2 with the MAC address of AP1 in the Remote MAC Address field.
  - Likewise, configure AP3 with the MAC address of AP1 in the Remote MAC Address field.

2. Verify the following for both access points:

- The LAN network configuration of the ADSL Modem Wireless Router and other AP device are configured to operate in the same LAN network address range as the LAN devices
- Both APs must be on the same LAN. That is, both the AP's LAN IP address must be in the same network.
- If using DHCP, both AP devices should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
- Both AP devices use the same SSID, Channel, authentication mode, if any, and encryption in use.

3. Verify connectivity across the LANs.

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

# Chapter 8

## Virtual Private Networking

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

This chapter is organized as follows:

- [“Overview of VPN Configuration” on page 8-2](#) provides an overview of the two most common VPN configurations: Client-to-Gateway and Gateway-to-Gateway.
- [“Planning a VPN” on page 8-4](#) 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 8-6](#) 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 8-7](#) 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 8-21](#) provides the steps needed to configure a VPN tunnel between two network gateways using the VPN Wizard.
- [“VPN Tunnel Control” on page 8-29](#) 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 8-38](#) 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.

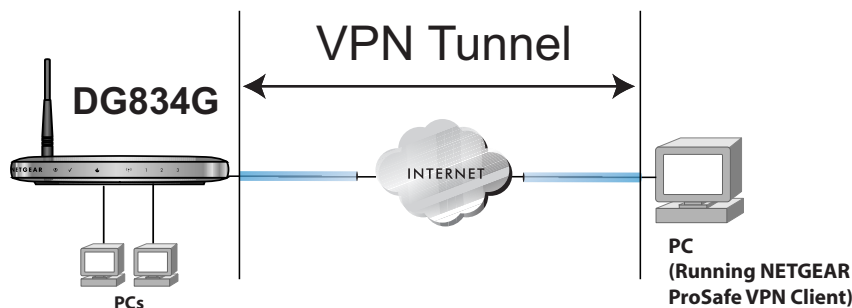
## Overview of VPN Configuration

---

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 DG834G v4 supports both of these types of VPN configurations. The ADSL Modem Wireless 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.

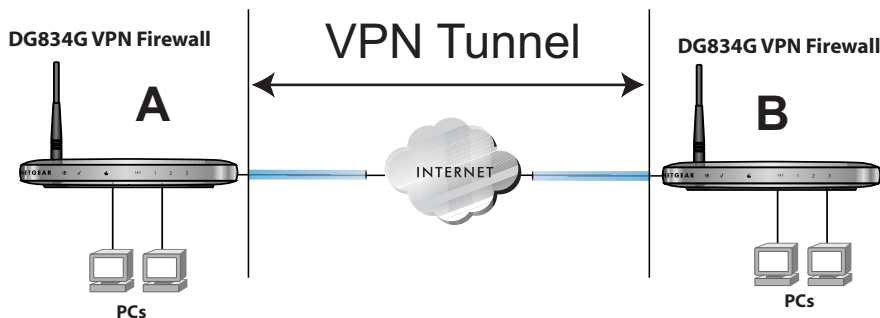


**Figure 8-1**

A VPN client access allows a remote PC to connect to your network from any location on the Internet. In this case, the remote PC is one tunnel endpoint, running the VPN client software. The ADSL Modem Wireless Router on your network is the other tunnel endpoint. See [“How to Set Up a Client-to-Gateway VPN Configuration” on page 8-7](#) to set up this configuration.

## Gateway-to-Gateway VPN Tunnels

- Gateway-to-Gateway VPN Tunnels provide secure access between networks, such as a branch or home office and a main office.



**Figure 8-2**

A VPN between two or more NETGEAR VPN-enabled routers is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use DG834G v4s on each end of the tunnel to form the VPN tunnel end points. See [“How to Set Up a Gateway-to-Gateway VPN Configuration”](#) on [page 8-21](#) 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 8-1. VPN Tunnel Configuration Worksheet**

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

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

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

- Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single PC?



- Will either endpoint use Fully Qualified Domain Names (FQDNs)? FQDNs supplied by Dynamic DNS providers (see [“The Use of a Fully Qualified Domain Name \(FQDN\)”](#) on [page B-8](#)) can allow a VPN endpoint with a dynamic IP address to initiate or respond to a tunnel request. Otherwise, the side using a dynamic IP address must always be the initiator.
- What method will you use to configure your VPN tunnels?
  - The VPN Wizard using VPNC defaults (see [Table 8-2](#))
  - The typical automated Internet Key Exchange (IKE) setup (see [“Using Auto Policy to Configure VPN Tunnels”](#) on [page 8-38](#))
  - A Manual Keying setup in which you must specify each phase of the connection (see [“Using Manual Policy to Configure VPN Tunnels”](#) on [page 8-48](#))?

**Table 8-2. Parameters Recommended by the VPNC and Used in the VPN Wizard**

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

- What level of IPSec VPN encryption will you use?
  - DES - The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
  - 3DES - (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- What level of authentication will you use?
  - MD5: 128 bits, faster but less secure.
  - SHA-1: 160 bits, slower but more secure.

## VPN Tunnel Configuration

---

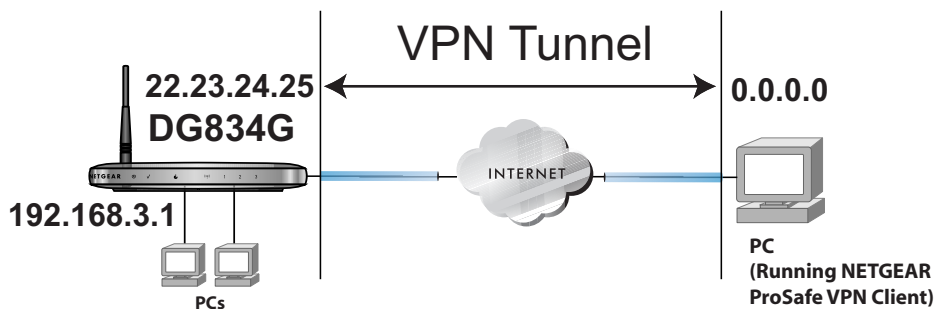
There are two tunnel configurations and three ways to configure them:

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
  - See “[How to Set Up a Client-to-Gateway VPN Configuration](#)” on page 8-7.
  - See “[How to Set Up a Gateway-to-Gateway VPN Configuration](#)” on page 8-21.
- See “[Using Auto Policy to Configure VPN Tunnels](#)” on page 8-38 when the VPN Wizard and its VPNC defaults (see [Table 8-2](#)) are not appropriate for your special circumstances, but you want to automate the Internet Key Exchange (IKE) setup.
- See “[Using Manual Policy to Configure VPN Tunnels](#)” on page 8-48 when the VPN Wizard and its VPNC defaults (see [Table 8-2](#)) are not appropriate for your special circumstances and you must specify each phase of the connection. You manually enter all the authentication and key parameters. You have more control over the process, however the process is more complex and there are more opportunities for errors or configuration mismatches between your DG834G v4 and the corresponding VPN endpoint gateway or client workstation.



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

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



**Figure 8-3**

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 DG834G v4](#)” on page 8-7 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 8-12 configures the NETGEAR ProSafe VPN Client endpoint.

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



**Note:** This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in [Table 8-2 on page 8-5](#). 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 8-38 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 8-4.

**Table 8-3. VPN Tunnel Configuration Worksheet**

Connection Name:	<b>RoadWarrior</b>			
Pre-Shared Key:	<b>12345678</b>			
Secure Association -- Main Mode or Manual Keys:	<b>Main</b>			
Perfect Forward Secrecy -- Enabled or Disabled:	<b>Disabled</b>			
Encryption Protocol -- DES or 3DES:	<b>3DES</b>			
Authentication Protocol -- MD5 or SHA-1:	<b>SHA-1</b>			
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	<b>Group 2</b>			
Key Life in seconds:	<b>28800 (8 hours)</b>			
IKE Life Time in seconds:	<b>3600 (1 hour)</b>			
VPN Endpoint	Local IPSec ID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
<b>Client</b>	<b>toDG834</b>	<b>—</b>	<b>—</b>	<b>Dynamic</b>
<b>DG834G v4</b>	<b>toClient</b>	<b>192.168.3.1</b>	<b>255.255.255.0</b>	<b>22.23.24.25</b>

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

1. Log in to the DG834G v4 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.

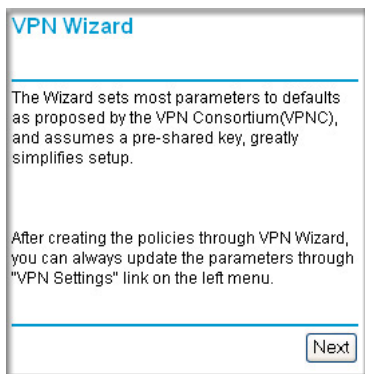


Figure 8-4

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

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

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

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

Figure 8-5

	<b>Tip:</b> The Connection Name is arbitrary and not relevant to how the configuration functions.
--	---

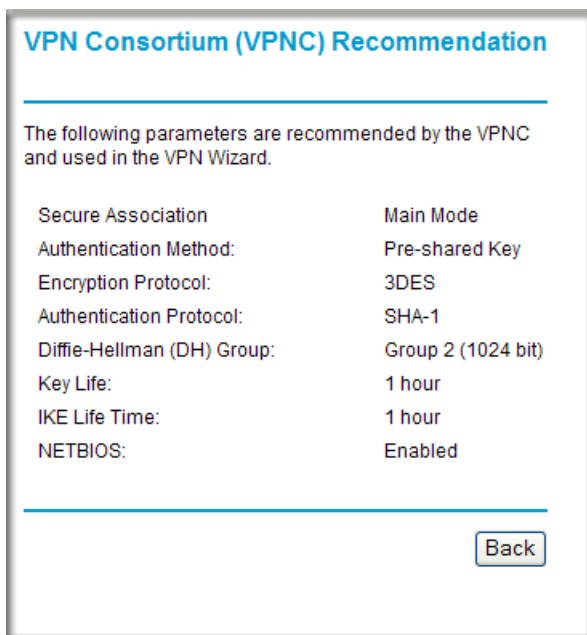
The Summary screen below displays.

The screenshot shows a web-based interface titled "VPN Wizard" with a "Summary" section. The interface is enclosed in a light gray border. The "Summary" section is separated from the rest of the page by a horizontal blue line. Below this line, the text "Please verify your inputs:" is followed by a list of configuration parameters. Each parameter is listed on the left, and its corresponding value is listed on the right. The parameters and their values are: Connection Name: RoadWarrior; Remote VPN Endpoint: Client PC; Remote Client Access: Single PC - no Subnet; Remote IP: Dynamic; Remote ID: (blank); Local Client Access: By subnet; Local IP: 192.168.3.1 / 255.255.255.0; Local ID: (blank). Below the list, there are two lines of text: "You can click [here](#) to view the VPNC-recommended parameters." and "Please click **\"Done\"** to apply the changes." At the bottom right of the form, there are three buttons: "Back", "Done", and "Cancel".

<b>VPN Wizard</b>	
<b>Summary</b>	
Please verify your inputs:	
Connection Name:	RoadWarrior
Remote VPN Endpoint:	Client PC
Remote Client Access:	Single PC - no Subnet
Remote IP:	Dynamic
Remote ID:	
Local Client Access:	By subnet
Local IP:	192.168.3.1 / 255.255.255.0
Local ID:	
You can click <a href="#">here</a> to view the VPNC-recommended parameters.	
Please click <b>\"Done\"</b> to apply the changes.	
<input type="button" value="Back"/> <input type="button" value="Done"/> <input type="button" value="Cancel"/>	

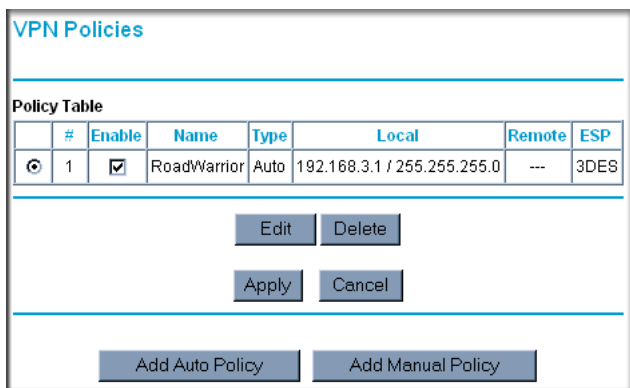
**Figure 8-6**

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



**Figure 8-7**

- Click **Done** on the Summary screen to complete the configuration procedure. The VPN Policies menu below displays showing that the new tunnel is enabled.



**Figure 8-8**

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



**Note:** Refer to [“Using Auto Policy to Configure VPN Tunnels”](#) on page 8-38 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.

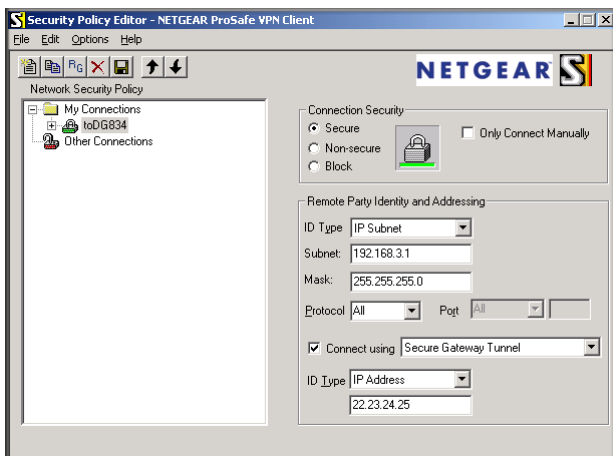


**Note:** Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

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.
  - a. Run the NETGEAR ProSafe Security Policy Editor program and, using the [“VPN Tunnel Configuration Worksheet”](#) on page 8-8, create a VPN Connection.





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



**Figure 8-9**

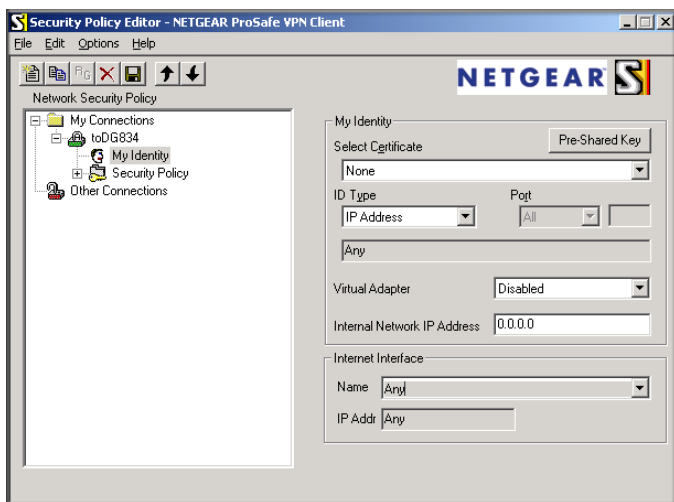
A “New Connection” listing appears in the list of policies. Rename the “New Connection” so that it matches the Connection Name you entered in the VPN Settings of the DG834G v4 on LAN A.

	<p><b>Note:</b> In this example, the Connection Name used on the client side of the VPN tunnel is <b>toDG834</b> and it does not have to match the <b>RoadWarrior</b> Connection Name used on the gateway side of the VPN tunnel because Connection Names are arbitrary to how the VPN tunnel functions.</p>
	<p><b>Tip:</b> Choose Connection Names that make sense to the people using and administering the VPN.</p>

- c. Select **Secure** in the Connection Security check-box group.
- d. Select **IP Subnet** in the ID Type menu.
- e. In this example, type **192.168.3.1** in the Subnet field as the network address of the DG834G v4.
- f. Enter **255.255.255.0** in the Mask field as the LAN Subnet Mask of the DG834G v4.
- g. Select **All** in the Protocol menu to allow all traffic through the VPN tunnel.



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



**Figure 8-11**

- b. Choose **None** in the Select Certificate menu.
- c. Select **IP Address** in the ID Type menu. If you are using a virtual fixed IP address, enter this address in the Internal Network IP Address box. Otherwise, leave this box empty.
- d. In the Internet Interface box, select the adapter you use to access the Internet. Select **PPP Adapter** in the Name menu if you have a dial-up Internet account. Select your Ethernet adapter if you have a dedicated Cable or DSL line. You may also choose Any if you will be switching between adapters or if you have only one adapter.

- e. Click the **Pre-Shared Key** button. In the Pre-Shared Key dialog box, click the **Enter Key** button. Enter the DG834G v4's Pre-Shared Key and click **OK**. In this example, **12345678** is entered. This field is case sensitive.

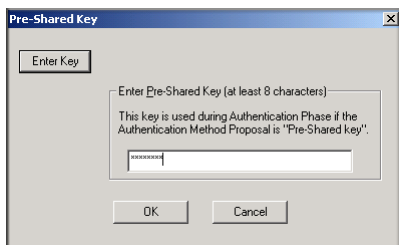


Figure 8-12

## 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 DG834G v4 configuration.

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

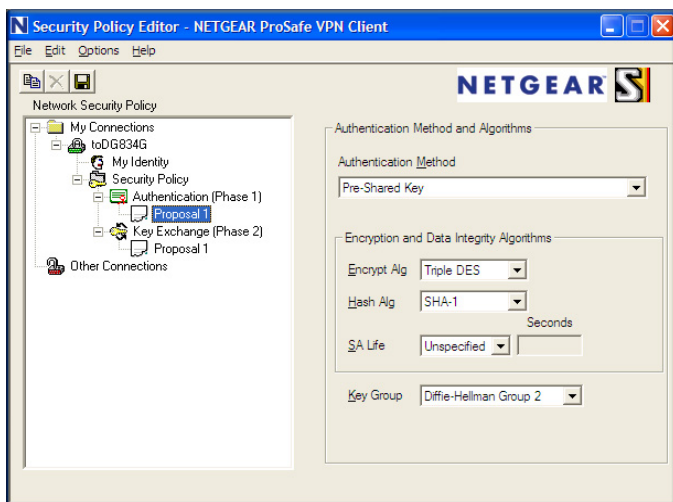
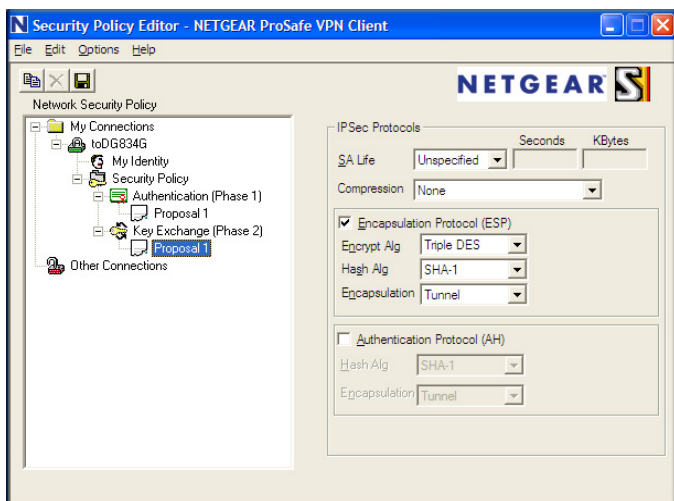


Figure 8-13

- c. In the Authentication Method menu, select **Pre-Shared key**.
  - d. In the Encrypt Alg menu, select the type of encryption to correspond with what was configured for the Encryption Protocol in the DG834G v4 in [Table 8-3 on page 8-8](#). 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 DG834G v4 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 8-14**

- b. In the SA Life menu, select **Unspecified**.
- c. In the Compression menu, select **None**.
- d. Check the Encapsulation Protocol (ESP) checkbox.
- e. In the Encrypt Alg menu, select the type of encryption to correspond with what was configured for the Encryption Protocol in the DG834G v4 in [Table 8-3 on page 8-8](#). 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 DG834G v4'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**.

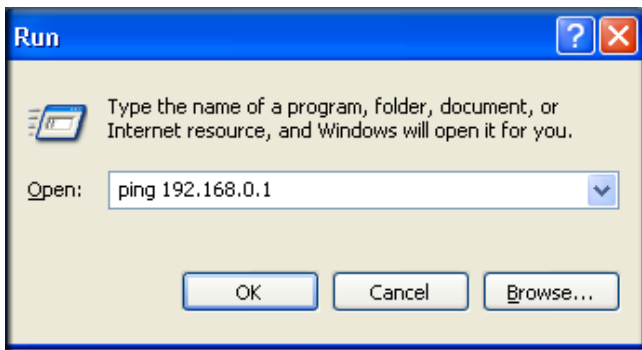


Figure 8-15

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

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

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

Figure 8-16

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

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

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

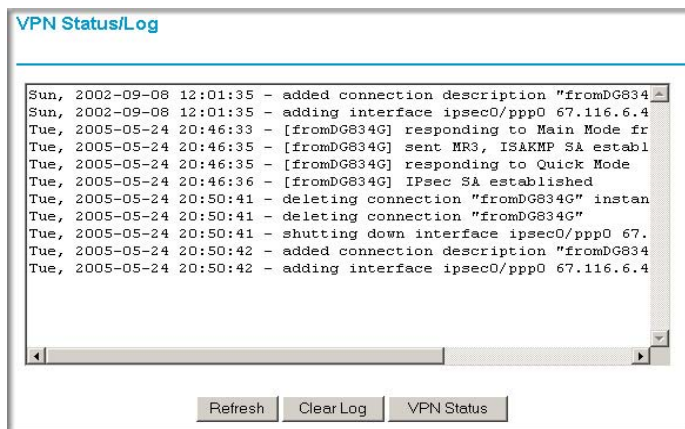


Figure 8-17



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

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

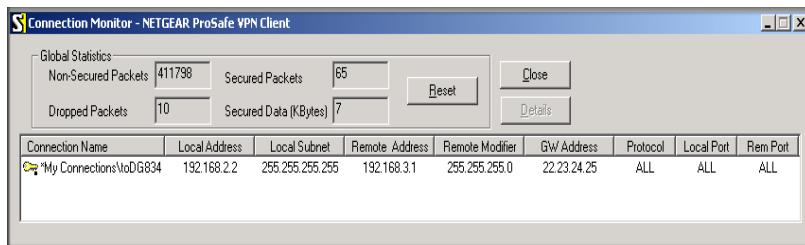


Figure 8-18

In this example you can see the following:

- The DG834G v4 has a public IP WAN address of 22.23.24.25.
- The DG834G v4 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.

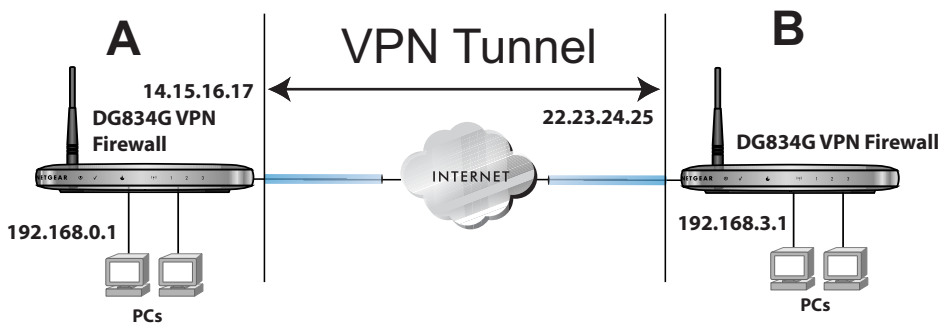


## How to Set Up a Gateway-to-Gateway VPN Configuration



**Note:** This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in [Table 8-2 on page 8-5](#). 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 8-38](#) to set up the VPN tunnel.

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



**Figure 8-19**

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

**Table 8-4. VPN Tunnel Configuration Worksheet**

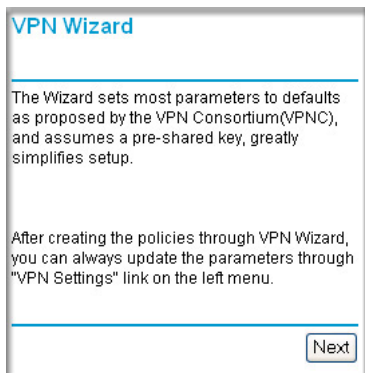
Connection Name:	<b>GtoG</b>			
Pre-Shared Key:	<b>12345678</b>			
Secure Association -- Main Mode or Manual Keys:	<b>Main</b>			
Perfect Forward Secrecy -- Enabled or Disabled:	<b>Disabled</b>			
Encryption Protocol -- DES or 3DES:	<b>3DES</b>			
Authentication Protocol -- MD5 or SHA-1:	<b>SHA-1</b>			
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	<b>Group 2</b>			
Key Life in seconds:	<b>28800 (8 hours)</b>			
IKE Life Time in seconds:	<b>3600 (1 hour)</b>			
				FQDN or Gateway IP (WAN IP Address)
VPN Endpoint	Local IPsec ID	LAN IP Address	Subnet Mask	
<b>DG834G v4_A</b>	<b>GW_A</b>	<b>192.168.0.1</b>	<b>255.255.255.0</b>	<b>14.15.16.17</b>
<b>DG834G v4_B</b>	<b>GW_B</b>	<b>192.168.3.1</b>	<b>255.255.255.0</b>	<b>22.23.24.25</b>



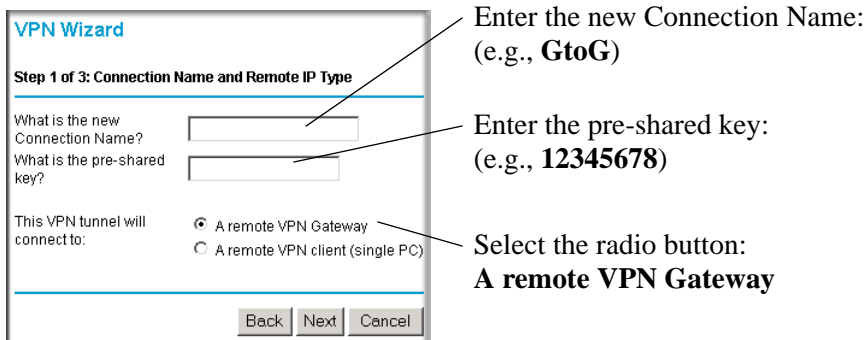
**Note:** The LAN IP address ranges of each VPN endpoint must be different. The connection will fail if both are using the NETGEAR default address range of 192.168.0.x.

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

1. Log in to the DG834G v4 on LAN A at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and password of **password**. Click the **VPN Wizard** link in the main menu to display this screen. Click **Next** to proceed.

**Figure 8-20**

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

**Figure 8-21**

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

**VPN Wizard**

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

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

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

**Figure 8-22**

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

**VPN Wizard**

**Step 3 of 3: Secure Connection Remote Accessibility**

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

IP Address:  .  .  .

Subnet Mask:  .  .  .

Enter the LAN IP settings of the remote VPN gateway:

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

**Figure 8-23**

The Summary screen below displays.

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

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

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

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

**Figure 8-24**

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the “**here**” link (see [Figure 8-24](#)). Click **Back** to return to the Summary screen.

### VPN Consortium (VPNC) Recommendation

---

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

Secure Association	Main Mode
Authentication Method:	Pre-shared Key
Encryption Protocol:	3DES
Authentication Protocol:	SHA-1
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)
Key Life:	1 hour
IKE Life Time:	1 hour
NETBIOS:	Enabled

---

**Figure 8-25**

- Click **Done** on the Summary screen (see [Figure 8-24](#)) to complete the configuration procedure. The VPN Settings menu below displays showing that the new tunnel is enabled.

### VPN Policies

---

**Policy Table**

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

---

**Figure 8-26**



**Note:** Refer to [“Using Auto Policy to Configure VPN Tunnels”](#) on page 8-38 to enable the IKE keepalive capability on an existing VPN tunnel.

6. Repeat for the DG834G v4 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 8-29 for information on the other ways.

- a. Open the DG834G v4 management interface and click on **VPN Status** to get the VPN Status/Log screen (Figure 8-27).

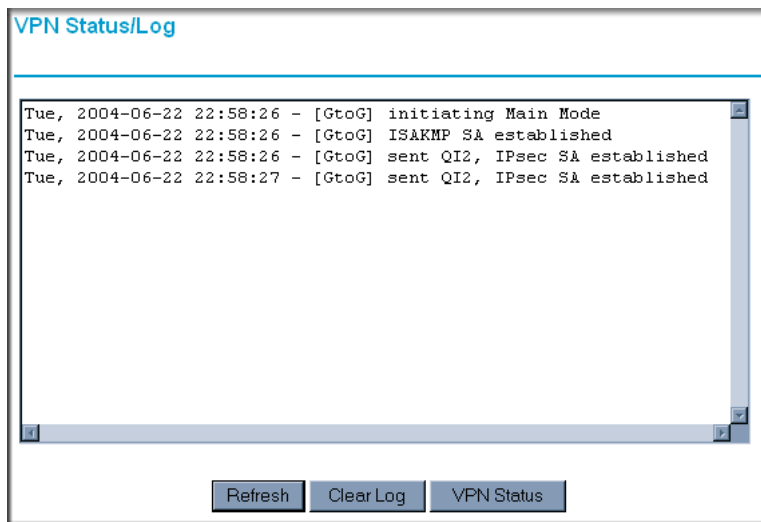


Figure 8-27

- b. Click on **VPN Status** (Figure 8-29) to get the Current VPN Tunnels (SAs) screen (Figure 8-28). Click on **Connect** for the VPN tunnel you want to activate.

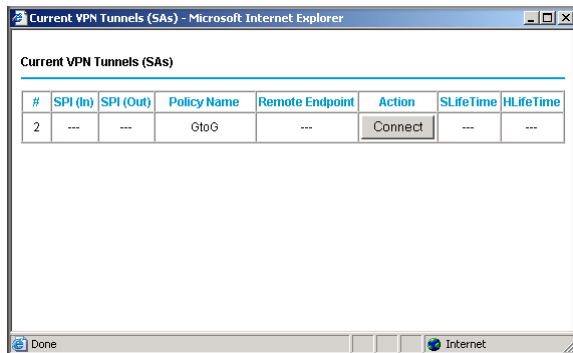


Figure 8-28

- c. Look at the VPN Status/Log screen (Figure 8-27) 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.

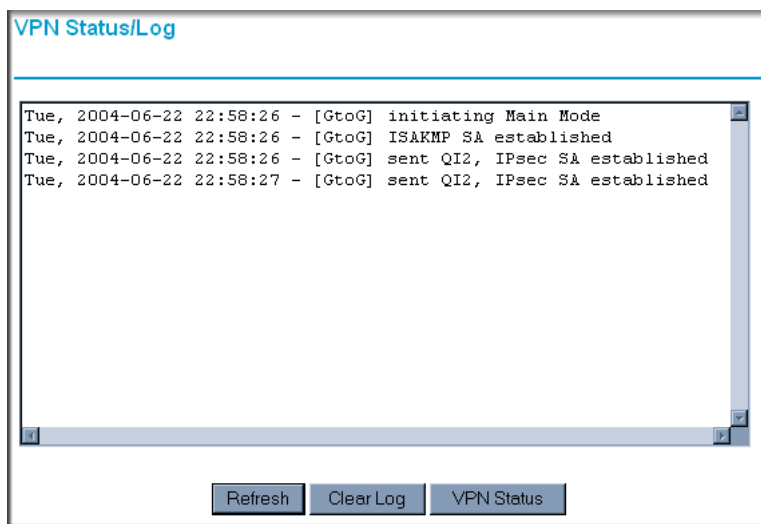


**Note:** Refer to [“Using Auto Policy to Configure VPN Tunnels”](#) on page 8-38 to enable the IKE keepalive capability on an existing VPN tunnel.

### Using the VPN Status Page to Activate a VPN Tunnel

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

1. Log in to the modem router.
2. Open the DG834G v4 management interface and click on **VPN Status** to get the VPN Status/Log screen ([Figure 8-29](#)).



**Figure 8-29**

3. Click on **VPN Status** (Figure 8-29) to get the Current VPN Tunnels (SAs) screen (Figure 8-30). Click on **Connect** for the VPN tunnel you want to activate.

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	aa185e44	af9bffc6	fromDG834G	66.120.188.152	Drop	3289	3287

Figure 8-30

### Activate the VPN Tunnel by Pinging the Remote Endpoint



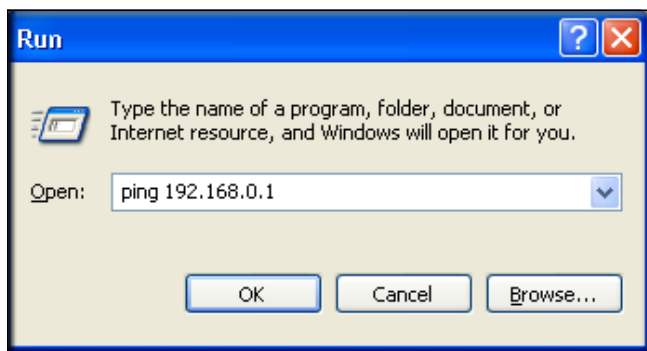
**Note:** This section uses 192.168.3.1 for an example remote endpoint LAN IP address.

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 DG834G v4'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.

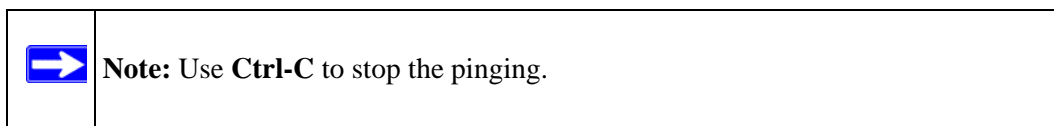
To perform a ping test using our example, start from the remote PC:

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



**Figure 8-31: Running a Ping test to the LAN from the PC**

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



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

**Figure 8-32**

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

- **Gateway-to-Gateway Configuration**—test the VPN tunnel by pinging the remote network from a PC attached to the DG834G v4.
  - a. Open command prompt (i.e., Start -> Run -> cmd).

- b. ping 192.168.3.1.

```
Pinging 192.168.3.1 with 32 bytes of data:  
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254  
Reply from 192.168.3.1: bytes=32 time=10ms TTL=254  
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254  
-
```

**Figure 8-33**



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

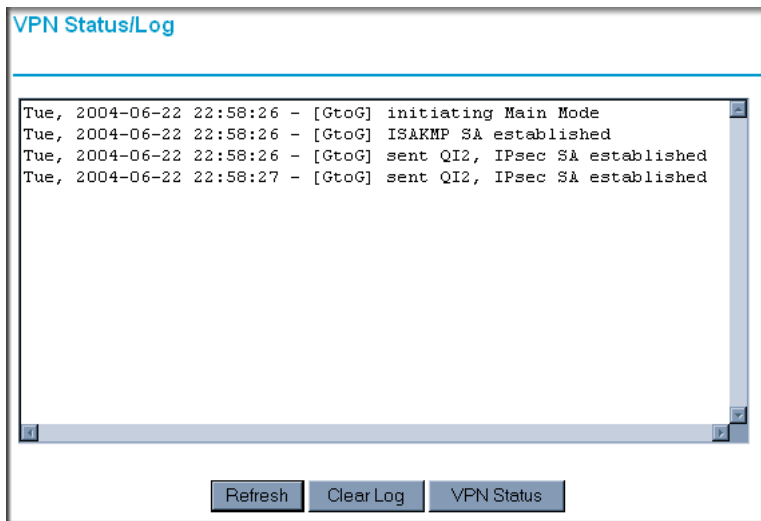
### **Start Using a VPN Tunnel to Activate It**

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

## Verifying the Status of a VPN Tunnel

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

1. Log in to the modem router.
2. Open the DG834G v4 management interface and click on **VPN Status** to get the VPN Status/Log screen (Figure 8-34).

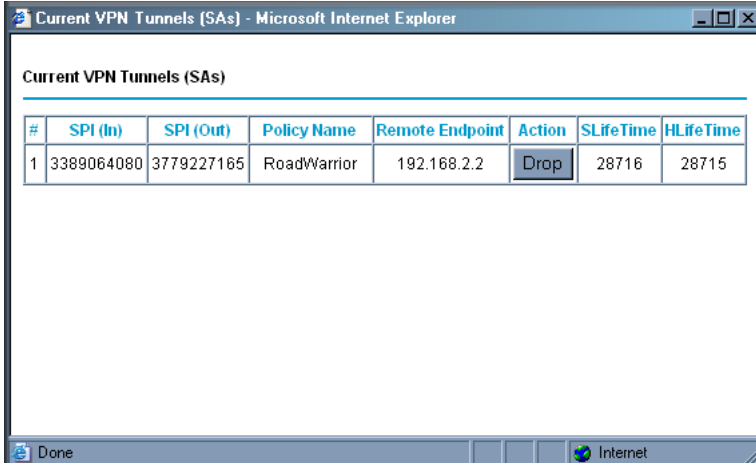


**Figure 8-34**

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.

3. Click on **VPN Status** (Figure 8-29) to get the Current VPN Tunnels (SAs) screen.



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

**Figure 8-35**

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

- **SPI**—each SA has a unique SPI (Security Parameter Index) for traffic in each direction. For "Manual" key exchange, the SPI is specified in the Policy definition. For "Automatic" key exchange, the SPI is generated by the IKE protocol.
- **Policy Name**—the 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.)

## Deactivating a VPN Tunnel

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

- Policy table on VPN Policies page
- VPN Status page

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

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

1. Log in to the modem router.
2. Open the DG834G v4 management interface and click on **VPN Policies** to get the VPN Policies screen (Figure 8-36).

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

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

Below the table are buttons for 'Edit', 'Delete', 'Apply', and 'Cancel'. At the bottom of the page are buttons for 'Add Auto Policy' and 'Add Manual Policy'.

**Figure 8-36**

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

### Using the VPN Status Page to Deactivate a VPN Tunnel

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

1. Log in to the modem router.

- Open the DG834G v4 management interface and click on **VPN Status** to get the VPN Status/Log screen (Figure 8-37).

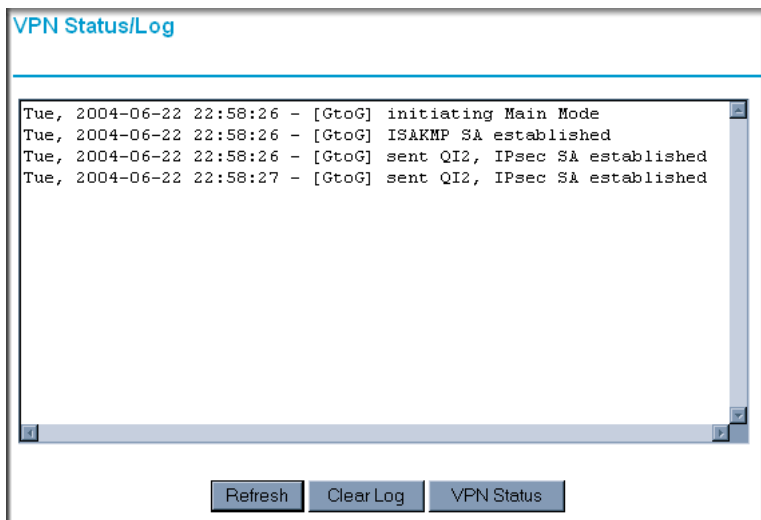


Figure 8-37

- Click **VPN Status** (Figure 8-37) to get the Current VPN Tunnels (SAs) screen (Figure 8-38). Click **Drop** for the VPN tunnel you want to deactivate.

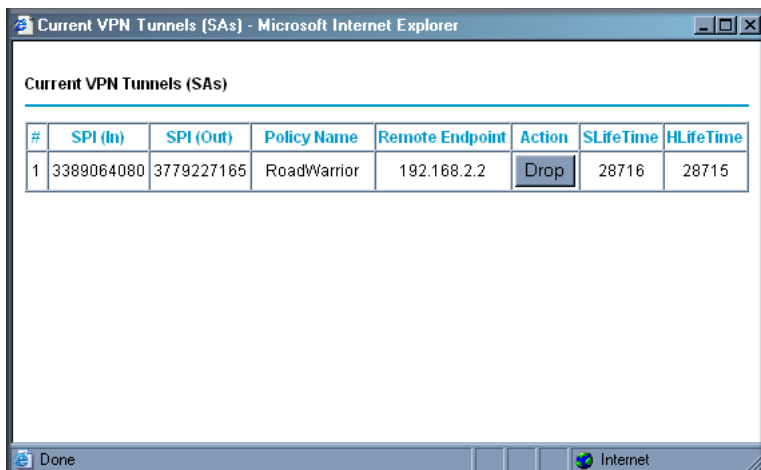


Figure 8-38



## Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the modem router.
2. Open the DG834G v4 management interface and click **VPN Policies** to display the VPN Policies screen (Figure 8-39). Select the radio button for the VPN tunnel to be deleted and click the **Delete** button.

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

Edit Delete

Apply Cancel

Add Auto Policy Add Manual Policy

Figure 8-39

## How to Set Up VPN Tunnels in Special Circumstances

---

When the VPN Wizard and its VPNC defaults (see [Table 8-2](#)) 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 8-38](#). 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 8-48](#). 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 DG834G v4 and the corresponding VPN endpoint gateway or client workstation.

### Using Auto Policy to Configure VPN Tunnels

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

See [“Example of Using Auto Policy” on page 8-43](#) for an example of using Auto Policy.

### Configuring VPN Network Connection Parameters

All VPN tunnels on the ADSL Modem Wireless 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 8-40](#).

**VPN Policies**

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

**VPN - Auto Policy**

**General**

Policy Name:

Remote VPN Endpoint: Address Type:  Address Data:

NetBIOS Enable

IKE Keep Alive

Ping IP Address:  .  .  .

**Local LAN**

IP Address:

Single/Start address:  .  .  .

Finish address:  .  .  .

Subnet Mask:  .  .  .

**Remote LAN**

IP Address:

Single/Start IP address:  .  .  .

Finish IP address:  .  .  .

Subnet Mask:  .  .  .

**IKE**

Direction:

Exchange Mode:

Diffie-Hellman (DH) Group:

Local Identity Type:  Data:

Remote Identity Type:  Data:

**Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-shared Key:

SA Life Time:  (Seconds)

Enable PFS (Perfect Forward Security)

Figure 8-40

The DG834G v4 VPN tunnel network connection fields are defined as follows:

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

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



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

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

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

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

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

**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.
- **Any**—any outgoing traffic from the "Local IP" computers will trigger an attempted VPN connection to the remote VPN endpoint. Please be sure you want this option before selecting it.

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

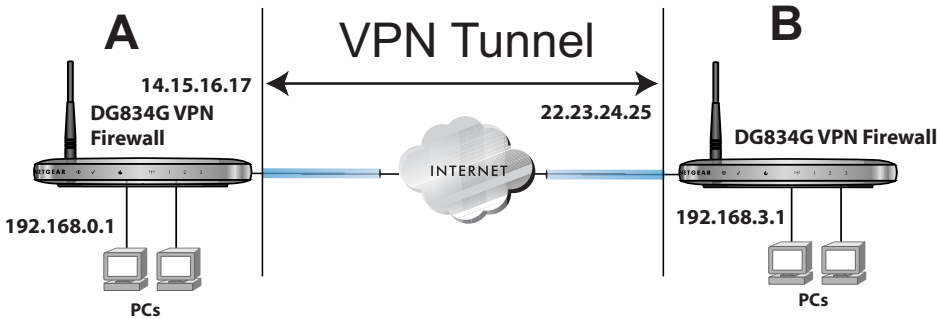


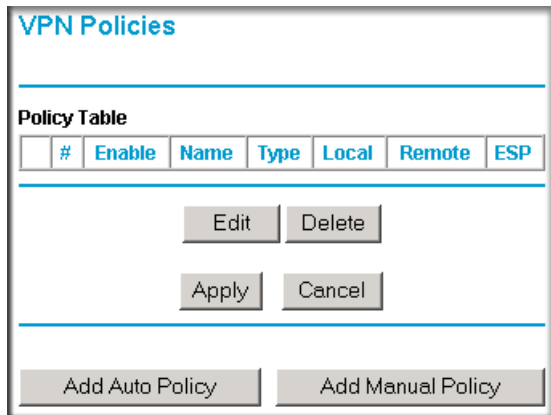
Figure 8-41

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

Table 8-5. VPN Tunnel Configuration Worksheet

Connection Name:	<b>GtoG</b>			
Pre-Shared Key:	<b>12345678</b>			
Secure Association -- Main Mode or Manual Keys:	<b>Main</b>			
Perfect Forward Secrecy -- Enabled or Disabled:	<b>Disabled</b>			
Encryption Protocol -- DES or 3DES:	<b>3DES</b>			
Authentication Protocol -- MD5 or SHA-1:	<b>SHA-1</b>			
Diffie-Hellman (DH) Group -- Group 1 or Group 2:	<b>Group 2</b>			
Key Life in seconds:	<b>28800 (8 hours)</b>			
IKE Life Time in seconds:	<b>3600 (1 hour)</b>			
				FQDN or Gateway IP (WAN IP Address)
VPN Endpoint	Local IPsec ID	LAN IP Address	Subnet Mask	
<b>DG834G v4 A</b>	<b>LAN_A</b>	<b>192.168.0.1</b>	<b>255.255.255.0</b>	<b>14.15.16.17</b>
<b>DG834G v4 B</b>	<b>LAN_B</b>	<b>192.168.3.1</b>	<b>255.255.255.0</b>	<b>22.23.24.25</b>

- Open the DG834G v4 on LAN A management interface and click on **VPN Policies**.



**Figure 8-42**

- Click **Add Auto Policy**.
- Enter policy settings (see [Figure 8-43](#)).
  - General
    - Policy Name = GtoG
    - Remote VPN Endpoint Address Type = Fixed IP Address
    - Remote VPN Endpoint Address Data = 22.23.24.25
  - Local LAN – use default setting
  - Remote LAN
    - IP Address = select Subnet address from the pulldown menu.
    - Start IP address = 192.168.3.1
    - Subnet Mask = 255.255.255.0
  - IKE
    - Direction = Initiator and Responder
    - Exchange Mode = Main Mode
    - Diffie-Hellman (DH) Group = Group 2 (1024 Bit)
    - Local Identity Type = use default setting
    - Remote Identity Type = use default setting
  - Parameters
    - Encryption Algorithm = 3DES



- Authentication Algorithm = MD5
- Pre-shared Key = 12345678

### VPN - Auto Policy

---

**General**

Policy Name:

Remote VPN Endpoint:  Address Type:  Address Data:

NetBIOS Enable

IKE Keep Alive

Ping IP Address:

---

**Local LAN**

IP Address:

Single/Start address:

Finish address:

Subnet Mask:

---

**Remote LAN**

IP Address:

Single/Start IP address:

Finish IP address:

Subnet Mask:

---

**IKE**

Direction:

Exchange Mode:

Diffie-Hellman (DH) Group:

Local Identity Type:

Data:

Remote Identity Type:

Data:

---

**Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-shared Key:

SA Life Time:  (Seconds)

Enable PFS (Perfect Forward Security)


Figure 8-43

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

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

**Figure 8-44**

6. Repeat for the DG834G v4 on LAN B and pay special attention to use the following network settings as appropriate.
- General, Remote Address Data (e.g., **14.15.16.17**)
  - Remote LAN, Start IP Address
    - IP Address (e.g, **192.168.0.1**)
    - Subnet Mask (e.g., **255.255.255.0**)
    - Preshared Key (e.g., **12345678**)
7. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

 **Note:** The VPN Status screen is only one of three ways to activate a VPN tunnel. See [“Activating a VPN Tunnel” on page 8-29](#) for information on the other ways.

- a. Open the DG834G v4 management interface and click on **VPN Status** to display the VPN Status/Log screen (Figure 8-45).

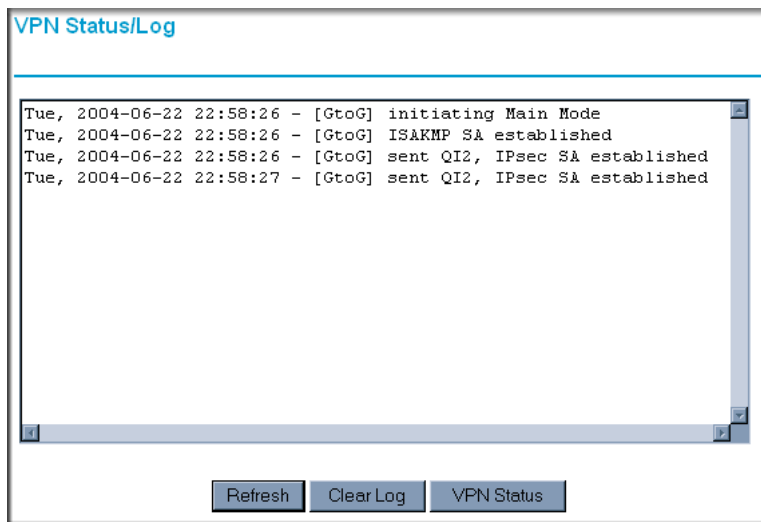


Figure 8-45

- b. Click **VPN Status** (Figure 8-45) to display the Current VPN Tunnels (SAs) screen (Figure 8-46). Click on **Connect** for the VPN tunnel you want to activate.

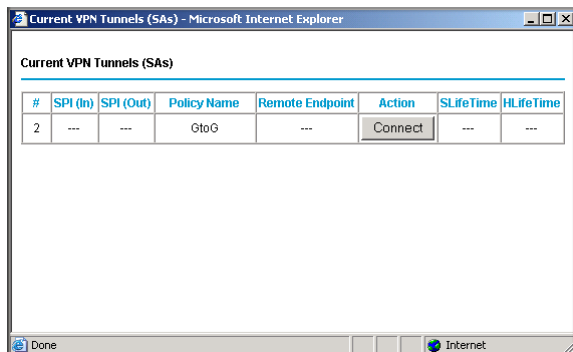


Figure 8-46

- c. Review the VPN Status/Log screen (Figure 8-45) to verify that the tunnel is connected.

## Using Manual Policy to Configure VPN Tunnels

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

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 8-47](#).

**VPN Policies**

**Policy Table**

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

Edit Delete

Apply Cancel

Add Auto Policy **Add Manual Policy**

---

**VPN - Manual Policy**

**General**

Policy Name:

Remote VPN Endpoint Address Type: Fixed IP Address

Address Data:

NETBIOS Enable

**Local LAN**

IP Address:  Subnet address

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

Finish address:  .  .  .

Subnet Mask: 255 . 255 . 255 . 0

**Remote LAN**

IP Address:  Single PC - no subnet

Single/Start IP address:  .  .  .

Finish IP address:  .  .  .

Subnet Mask:  .  .  .

**ESP Configuration**

SPI - Incoming:  (Hex, 3 Characters)

SPI - Outgoing:  (Hex, 3 Characters)

Encryption: 3DES

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

Authentication: SHA-1

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

Back Apply Cancel

Figure 8-47

**General.** The DG834G v4 VPN tunnel network connection fields are defined as follows:

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



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

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

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

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.

- **Any**—any outgoing traffic from the “Local IP” computers will trigger an attempted VPN connection to the remote VPN endpoint. Please be sure you want this option before selecting it.

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 9

## Troubleshooting

This chapter gives information about troubleshooting your 54 Mbps ADSL Modem Wireless Router Model DG834G. 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 9-1](#).
- I can’t access the router’s configuration with my browser.  
Go to [“Troubleshooting the Web Configuration Interface” on page 9-3](#).
- I’ve configured the router but I can’t access the Internet.  
Go to [“Troubleshooting the ISP Connection” on page 9-4](#).
- I can’t remember the router’s configuration password.  
Go to [“Restoring the Default Configuration and Password” on page 9-9](#).
- I want to clear the configuration and start over again.  
Go to [“Restoring the Default Configuration and Password” on page 9-9](#).

### Basic Functioning

---

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

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

- c. The WAN port LED is lit.

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

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

## Power LED Not On

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

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

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

## Test LED Never Turns On or Test LED Stays On

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

If you experience problems with the Test LED:

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

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

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

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

## LAN or Internet Port LEDs Not On

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



- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
  - When connecting the router’s WAN ADSL port, use the cable that was supplied with the DG834G v4.

## Troubleshooting the Web Configuration Interface

---

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

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



**Note:** If your computer’s IP address is shown as 169.254.x.x:  
Recent versions of Windows and MacOS 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 9-9](#).
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

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

## Troubleshooting the ISP Connection

---

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

### ADSL link

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

#### Internet LED Green or Blinking Green

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

#### Internet LED Blinking Amber

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

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

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

## Internet LED Off

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

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

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

## Obtaining a WAN IP Address

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

To check the WAN IP address from the browser interface:

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

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

- Your ISP may require a Multiplexing Method or Virtual Path Identifier/Virtual Channel Identifier parameter.  
Verify with your ISP the Multiplexing Method and parameter value, and update the router's ADSL Settings accordingly.
- Your ISP may require a login program.  
Ask your ISP whether they require PPP over Ethernet (PPPoE) or PPP over ATM (PPPOA) login.

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

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

OR

Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu. Refer to the *ADSL Modem Wireless Router Setup Manual* (see [Table 3-1 on page 3-1](#)).

## Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

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

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



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

## Troubleshooting Internet Browsing

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

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

## Troubleshooting a TCP/IP Network Using the Ping Utility

---

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

### Testing the LAN Path to Your Router

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

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

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

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in [“LAN or Internet Port LEDs Not On”](#) on page 9-2.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

## Testing the Path from Your Computer to a Remote Device

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

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

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

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

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

- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to “clone” or “spoof” the MAC address from the authorized PC. Refer to your *ADSL Modem Wireless Router Setup Manual* (see [Table 3-1 on page 3-1](#)).

## Restoring the Default Configuration and Password

---

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

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

### Using the Reset button

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

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

## Problems with Date and Time

---

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

- 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 54 Mbps ADSL Modem Wireless Router Model DG834G.

### Network Protocol and Standards Compatibility

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

### Power Adapter

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

### Physical Specifications

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

### Environmental Specifications

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

### Electromagnetic Emissions

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

### Interface Specifications

LAN: 10BASE-T or 100BASE-Tx, RJ-45  
WAN: ADSL, ADSL2+, Dual RJ-11, pins 2 and 3, T1.413, G.DMT, G.Lite, ITU Annex A (for the DG834G) or ITU Annex B (for the DG834GB)

---



# Appendix B

## NETGEAR VPN Configuration

### DG834G v4 to FVL328

---

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DG834G v4 to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>).

### Configuration Profile

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

**Table B-1. Profile Summary**

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

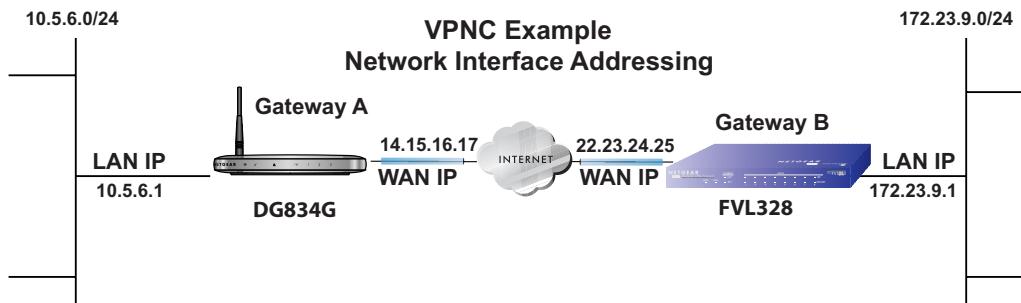


Figure B-1



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

## Step-By-Step Configuration

1. Configure the DG834G v4 as in the Gateway-to-Gateway procedures using the VPN Wizard (see “[How to Set Up a Gateway-to-Gateway VPN Configuration](#)” on page 8-21), being certain to use appropriate network addresses for the environment.

The LAN Addresses used in this example are as follows:

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

- a. 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.
- c. In Step 3, enter the following:
  - IP Address = **172.23.9.1**
  - Subnet Mask = **255.255.255.0**

**VPN Policies**

Policy Table

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

**Click VPN Policies under Advanced - VPN to invoke this screen**

**VPN - Auto Policy**

**General**

Policy Name: toFVL328

Remote VPN Endpoint: Fixed IP Address

Address Data: 66.170.188.152  
22.23.24.25

NetBIOS Enable  
 IKE Keep Alive

Ping IP Address: . . . .

**Local LAN**

IP Address: Subnet address

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

Finish address: . 10 . 5 . 6 . 1

Subnet Mask: 255 . 255 . 255 . 0

**Remote LAN**

IP Address: Subnet address

Single/Start IP address: 192 . 168 . 2 . 1

Finish IP address: . 172 . 23 . 9 . 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: WAN IP Address

Data: n/a

Remote Identity Type: IP Address

Data: n/a

**Parameters**

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Pre-shared Key: 12345678

SA Life Time: 28800 (Seconds)

Enable PFS (Perfect Forward Security)

Figure B-2

2. Configure the FVL328 as in the Gateway-to-Gateway procedures for the VPN Wizard (see [“How to Set Up a Gateway-to-Gateway VPN Configuration”](#) on page 8-21), 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**

**IKE Policies**

Policy Table							
#	Name	Mode	Local ID	Remote ID	Encr	Auth	DH
<input checked="" type="checkbox"/>	1	toDG834	Main	22.23.24.25	14.15.16.17	3DES	SHA1 Group 2 (1024 Bit)

Buttons: Add, Edit, Delete, Cancel

Click IKE Policies under VPN to invoke this screen

**IKE Policy Configuration**

**General**  
 Policy Name: jim2in toDG834  
 Direction/Type: Both Directions  
 Exchange Mode: Main Mode

**Local**  
 Local Identity Type: WAN IP Address  
 Local Identity Data: 67.125.91.84  
 22.23.24.25

**Remote**  
 Remote Identity Type: Remote WAN IP  
 Remote Identity Data: 67.125.91.84  
 14.15.16.17

**IKE SA Parameters**  
 Encryption Algorithm: 3DES  
 Authentication Algorithm: SHA-1  
 Authentication Method:  Pre-shared Key  
 \*\*\*\*\*  
 RSA Signature (requires Certificate)  
 Certificate: Group 2 (1024 Bit)  
 SA Life Time: 28800 (secs)

Buttons: Back, Apply, Cancel

**VPN Policies**

#	Enable	Name	Type	Local	Remote	AH	ESP
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1 jim2james	Auto	192.168.0.1/255.255.255.0	192.168.0.1/255.255.255.0	Disabled	ESP

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

Click VPN Policies under VPN to invoke this screen

**VPN - Auto Policy**

**General**  
 Policy Name: jim2james  
 IKE policy: toDG834  
 IKE Keep Alive  
 Remote VPN Endpoint: toDG834  
 Address Type: IP Address  
 Address Data: 67.125.91.84  
 SA Life Time: 86400 (seconds)  
 0 (bytes)  
 IPsec PFS  
 NetBIOS Enable  
 PFS Key Group: Group 1 (768 Bit)

**Traffic Selector**  
**Local IP**  
 Subnet address: [dropdown]  
 Start IP address: 192.168.0.1  
 Finish IP address: 0.172.23.9  
 Subnet Mask: 255.255.255.0  
**Remote IP**  
 Subnet address: [dropdown]  
 Start IP address: 192.168.0.1  
 Finish IP address: 0.10.5.6  
 Subnet Mask: 255.255.255.0

**AH Configuration**  
 Enable Authentication  
 Authentication Algorithm: MD5

**ESP Configuration**  
 Enable Encryption  
 Enable Authentication  
 Encryption Algorithm: 3DES  
 Authentication Algorithm: SHA-1

Buttons: Back, Apply, Cancel

Figure B-3

3. Test the VPN tunnel by pinging the remote network from a PC attached to the DG834G v4.
  - a. Open the command prompt (Start -> Run -> cmd)
  - b. ping 172.23.9.1

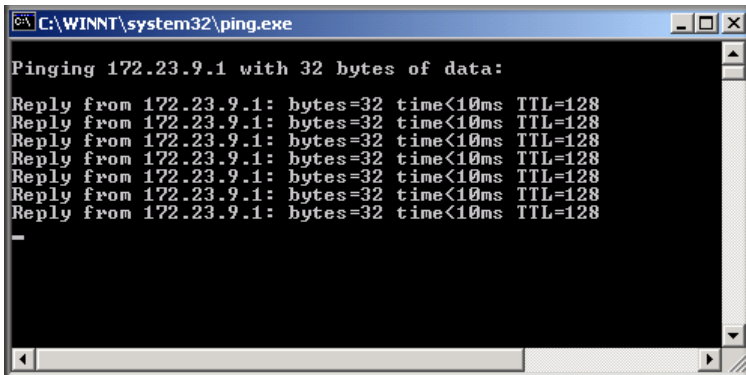



Figure B-4

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

---

## DG834G v4 with FQDN to FVL328

---

This appendix is a case study on how to configure a VPN tunnel from a NETGEAR DG834G v4 to a FVL328 using a Fully Qualified Domain Name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>).

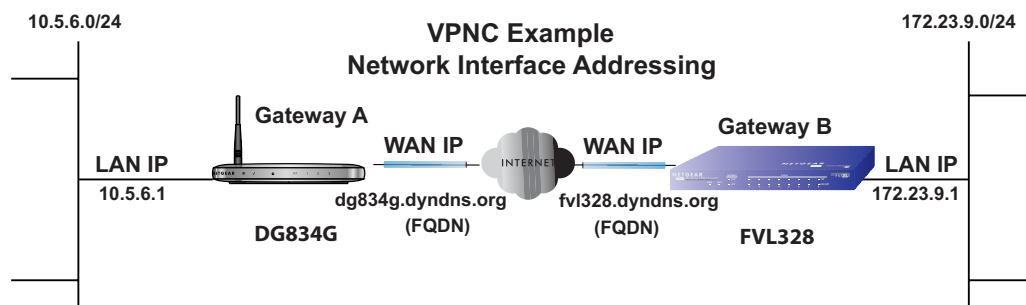
### Configuration Profile

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



**Table B-2. Profile Summary**

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

**Figure B-5**

**Note:** Product updates are available on the NETGEAR, Inc. web site at <http://kbserver.netgear.com/DG834G v4.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 3<sup>rd</sup> 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](http://www.dyndns.org)
- TZO.com: [netgear.tzo.com](http://netgear.tzo.com)
- ngDDNS: [ngddns.iego.net](http://ngddns.iego.net)

In this example, Gateway A is configured using an example FQDN provided by a DDNS Service provider. In this case we established the hostname **dg834g.dyndns.org** for gateway A using the DynDNS service. Gateway B 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.

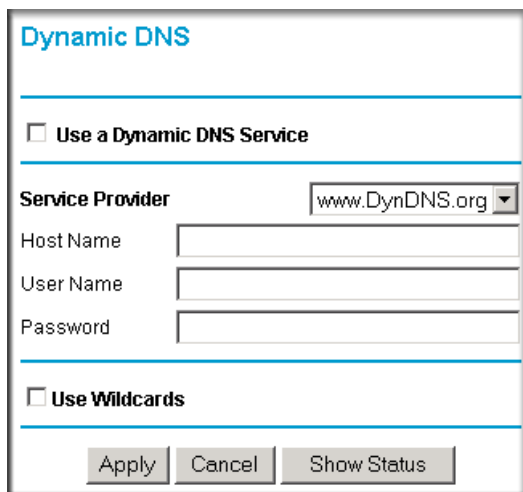
## Step-By-Step Configuration

1. Log in to the DG834G v4 labeled Gateway A as in the illustration.

Out of the box, the DG834G v4 is set for its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**. 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.

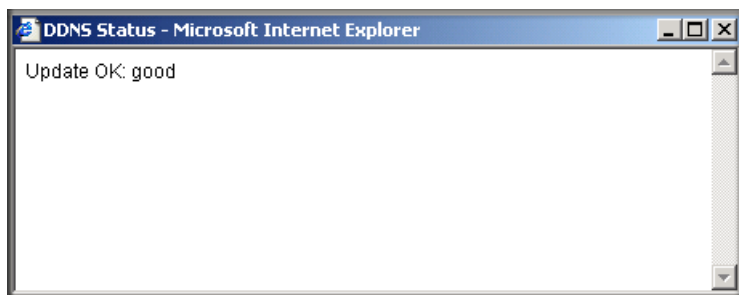
3. On the DG834G v4, configure the Dynamic DNS settings.
  - a. Browse to the Dynamic DNS Setup Screen (see [Figure B-6](#)) in the Advanced menu.



The image shows a web browser window titled "Dynamic DNS". At the top, there is a checkbox labeled "Use a Dynamic DNS Service". Below this, there is a "Service Provider" dropdown menu with "www.DynDNS.org" selected. Underneath are three text input fields labeled "Host Name", "User Name", and "Password". At the bottom of the form, there is another checkbox labeled "Use Wildcards". Below the form are three buttons: "Apply", "Cancel", and "Show Status".

**Figure B-6**

- b. Configure this screen with appropriate account and hostname settings and then click **Apply**.
  - Check the box **Use a Dynamic DNS Service**.
  - Host Name = dg834g.dyndns.org
  - User Name = <user's account username>
  - Password = <user's account password>
- c. Click **Show Status**. The resulting screen should show Update OK: good (see [Figure B-7](#)).



**Figure B-7**

4. On the FVL328, configure the Dynamic DNS settings. Assume a properly configured DynDNS account.
  - a. Browse to the Dynamic DNS Setup Screen (see [Figure B-8](#)) in the Advanced menu.



**Figure B-8**

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

**Dynamic DNS**

---

**Use a dynamic DNS service**

None

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

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

ngDDNS [Click here to register](#)

---

**DynDNS**

Host and Domain Name

  
example: yourname.dyndns.org

User Name

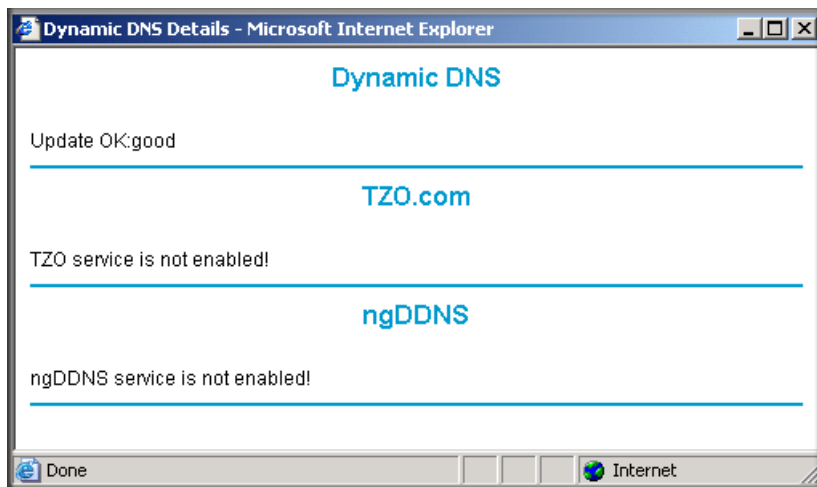
Password

Use wildcards

---

**Figure B-9**

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

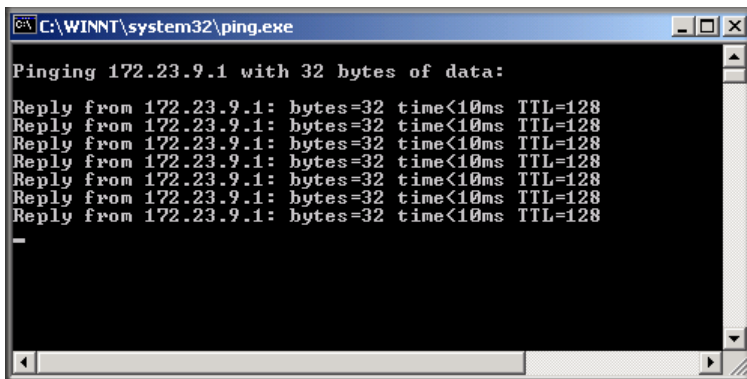
**Figure B-10**

5. Configure the DG834G v4 as in the Gateway-to-Gateway procedures using the VPN Wizard (see [“How to Set Up a Gateway-to-Gateway VPN Configuration” on page 8-21](#)), being certain to use appropriate network addresses for the environment.

The LAN Addresses used in this example are as follows:

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

- a. In Step 1, enter **toFVL328** for the Connection Name.
  - b. In Step 2, enter **fv1328.dyndns.org** for the remote WAN's IP address.
  - c. 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 8-21](#)), 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 **dg834g.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 DG834G v4.
    - a. Open the command prompt (Start -> Run -> cmd)
    - b. ping 172.23.9.1



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

Pinging 172.23.9.1 with 32 bytes of data:

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

Figure B-11



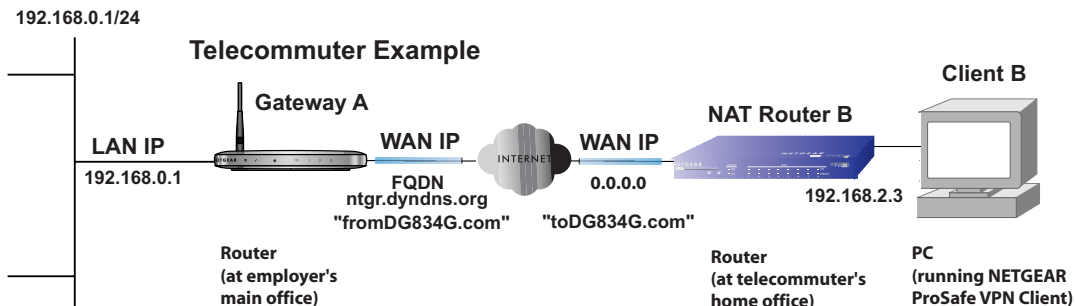
**Note:** The pings may fail the first time. If this happens, try the pings a second time.

## Configuration Summary (Telecommuter Example)

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

**Table B-3. Configuration summary (telecommuter example)**

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



**Figure B-12**

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

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

- [Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office.](#)



- [Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office](#) configures the NETGEAR ProSafe VPN Client endpoint.

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

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

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

**VPN - Auto Policy**

**General**

Policy Name: fromDG834G

Remote VPN Endpoint Address Type: Dynamic IP address

Address Data: n/a

NetBIOS Enable

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

**Local LAN**

IP Address Subnet address

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

Finish address: . . . .

Subnet Mask: 255 . 255 . 255 . 0

**Remote LAN**

IP Address Single address

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

Finish IP address: . . . .

Subnet Mask: . . . .

**IKE**

Direction: Responder only

Exchange Mode: Main Mode

Diffie-Hellman (DH) Group: Auto

Local Identity Type: Fully Qualified Domain Name

Data: fromDG834G.com

Remote Identity Type: Fully Qualified Domain Name

Data: toDG834G.com

**Parameters**

Encryption Algorithm: 3DES

Authentication Algorithm: Auto

Pre-shared Key: 12345678

SA Life Time: 3600 (seconds)

Enable PFS (Perfect Forward Security)


Buttons: Back, Apply, Cancel

**Annotations:**

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

Figure B-13

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



**VPN Policies**

**Policy Table**

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

Edit Delete

Apply Cancel

Add Auto Policy Add Manual Policy

**Figure B-14**

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


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

This procedure describes how to configure the 54 Mbps ADSL Modem Wireless Router Model DG834G. 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 54 Mbps ADSL Modem Wireless Router Model DG834G software, be sure to turn off any virus protection or firewall software you may be running on your PC.

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

- b. From the **Edit** menu of the **Security Policy Editor**, click **Add**, then **Connection**. A **New Connection** listing appears in the list of policies. Rename the **New Connection** so that it matches the **Connection Name** you entered in the **VPN Settings** of the DG834G v4 on Gateway A.



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



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

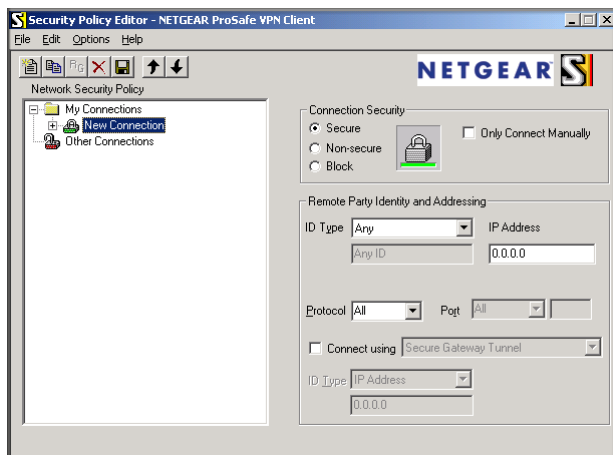
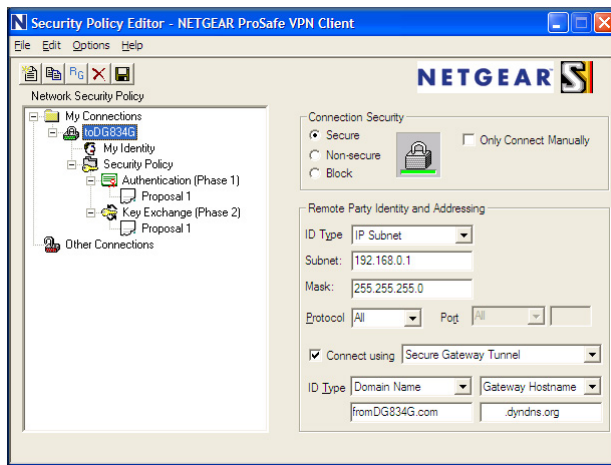


Figure B-15

**Figure B-16**

- c. Select **Secure** in the **Connection Security** check-box group.
  - 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 DG834G v4.
  - f. Enter **255.255.255.0** in the Mask field as the **LAN Subnet Mask** of the DG834G v4.
  - g. Select **All** in the **Protocol** menu to allow all traffic through the VPN tunnel.
  - h. Select the **Connect using Secure Gateway Tunnel** check box.
  - i. Select **Domain Name** in the **ID Type** menu below the check box and enter **fromDG834G.com** (in this example).
  - j. Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).
  - k. The resulting Connection Settings are shown in [Figure B-16](#).
3. Configure the **Security Policy** in the 54 Mbps ADSL Modem Wireless Router Model DG834G software.
    - a. In the **Network Security Policy** list, expand the new connection by double clicking its name or clicking on the “+” symbol. **My Identity** and **Security Policy** subheadings appear below the connection name.

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

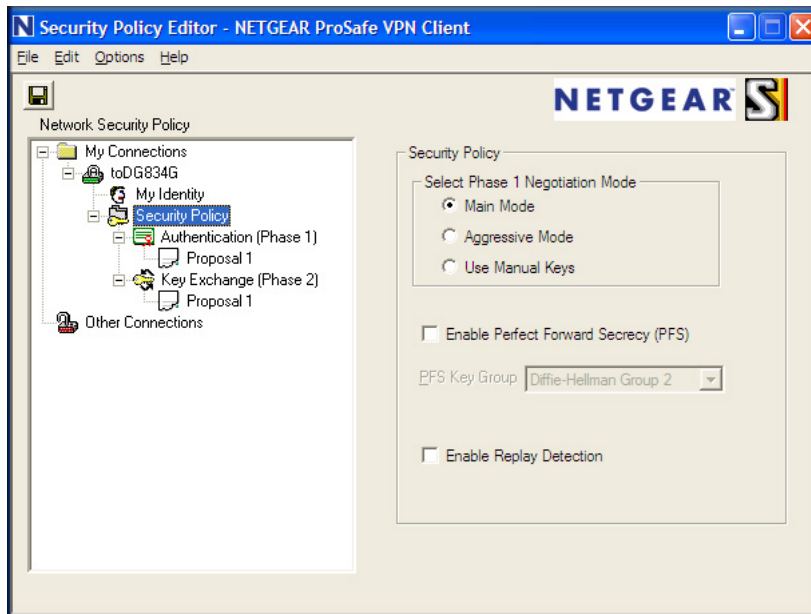
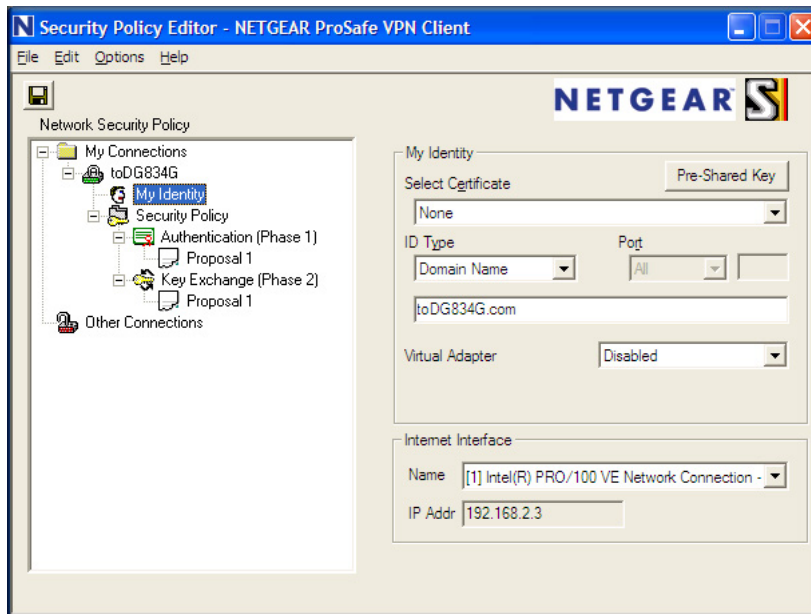


Figure B-17

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

In this step, you will provide information about the remote VPN client PC. You will need to provide the Pre-Shared Key that you configured in the DG834G v4 and either a fixed IP address or a “fixed virtual” IP address of the VPN client PC.

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

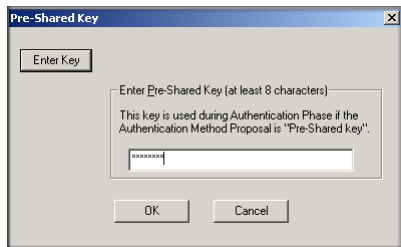


**Figure B-18**

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



- e. Click the **Pre-Shared Key** button.

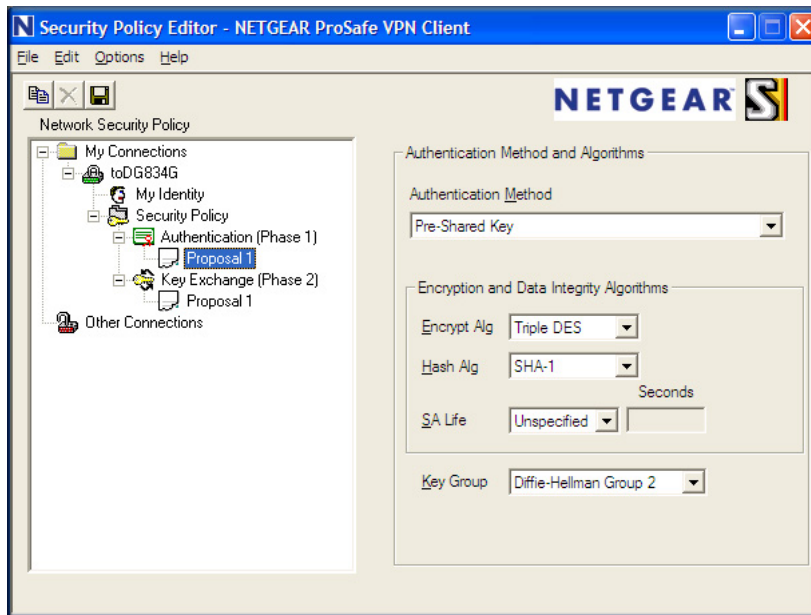


**Figure B-19**

- f. In the **Pre-Shared Key** dialog box, click the **Enter Key** button. Enter the DG834G v4's **Pre-Shared Key** and click **OK**. In this example, **12345678** is entered. This field is case sensitive.
5. Configure the **VPN Client Authentication Proposal**.

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

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

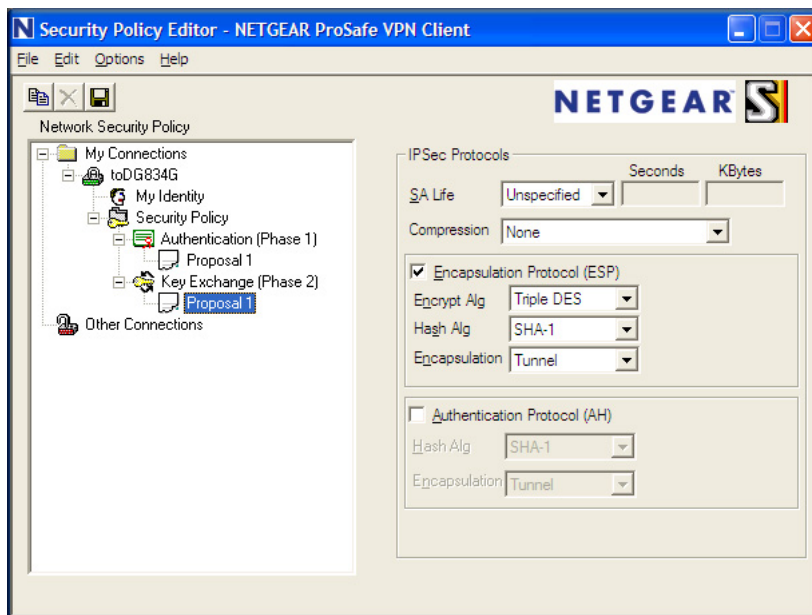


**Figure B-20**

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

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

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



**Figure B-21**

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

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

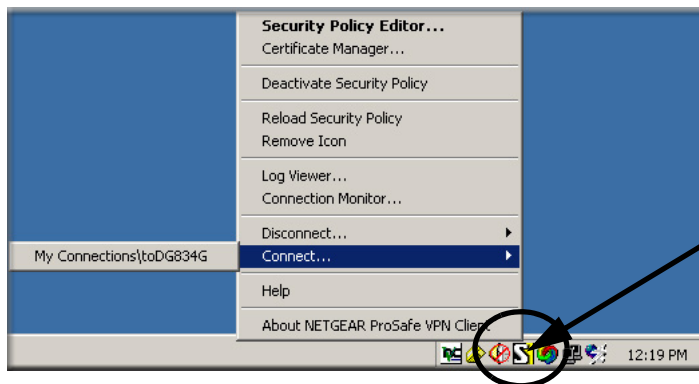
After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router’s LAN.

8. Check the **VPN Connection**.

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

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

The 54 Mbps ADSL Modem Wireless Router Model DG834G 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.



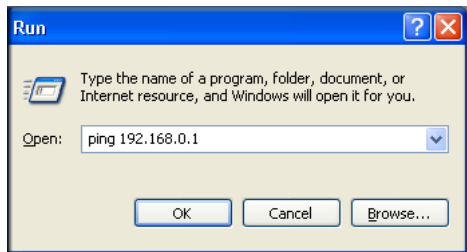
Right-mouse-click on the system tray icon to open the popup menu.

**Figure B-22**

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

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

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



**Figure B-23**

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

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

**Figure B-24**

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




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

## Monitoring the VPN Tunnel (Telecommuter Example)

### Viewing the PC Client's Connection Monitor and Log Viewer

To view information on the progress and status of the VPN client connection, open the 54 Mbps ADSL Modem Wireless Router Model DG834G **Log Viewer**.

1. To launch this function, click on the Windows **Start** button, then select **Programs**, then **54 Mbps ADSL Modem Wireless Router Model DG834G**, then **Log Viewer**.

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

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

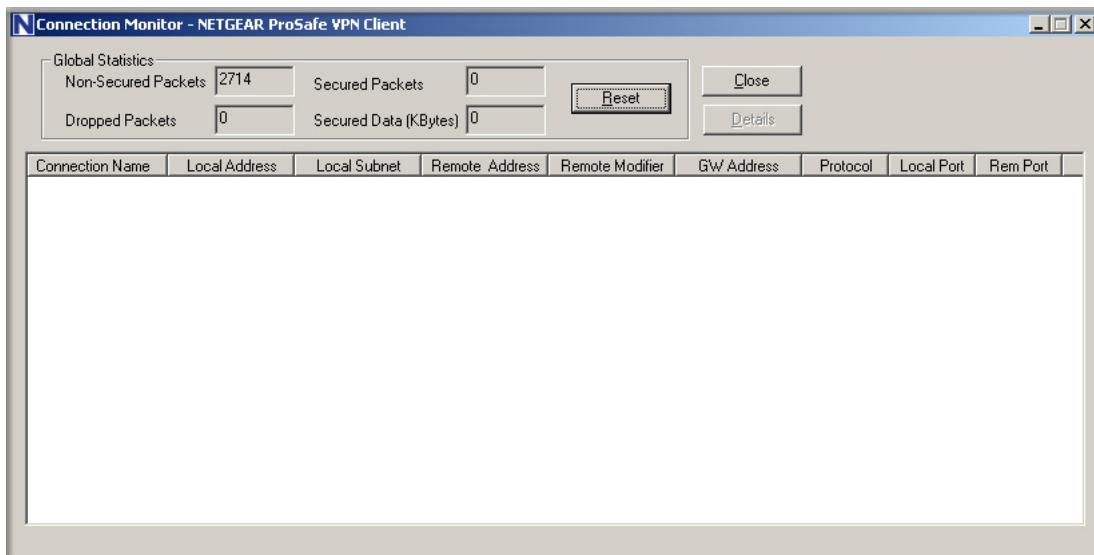


Figure B-25

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



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

## Viewing the VPN Router's VPN Status and Log Information

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

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

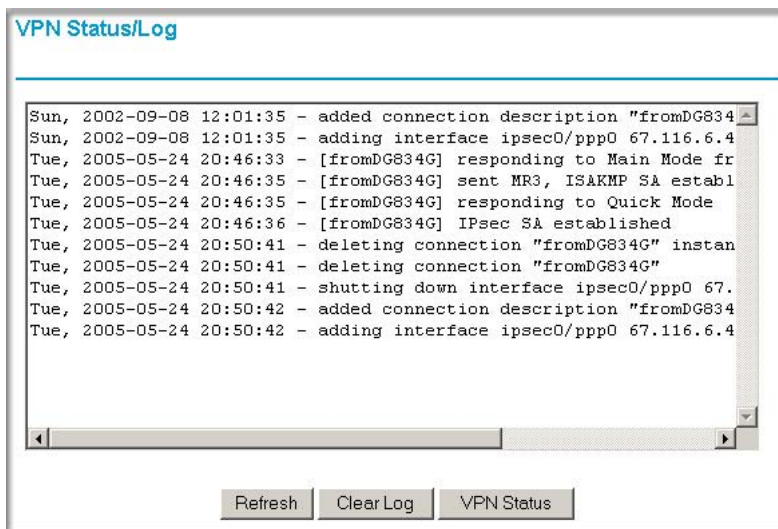
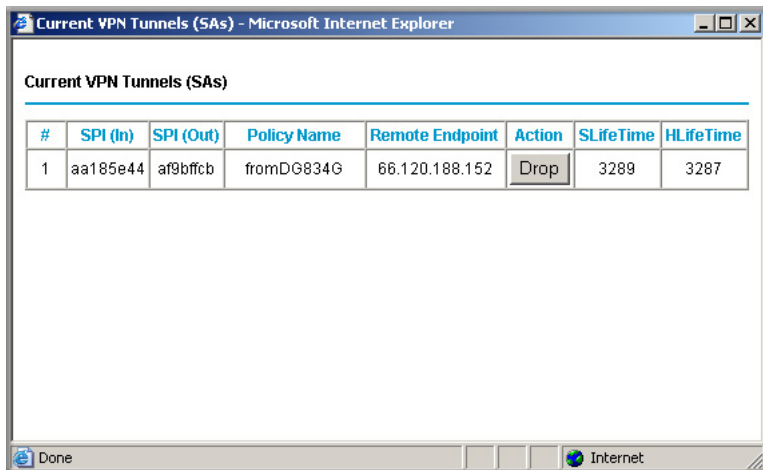


Figure B-26

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



The screenshot shows a web browser window titled "Current VPN Tunnels (SAs) - Microsoft Internet Explorer". The main content area displays a table with the following data:

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	aa185e44	af9bffc3	fromDG834G	66.120.188.152	Drop	3289	3287

The browser's status bar at the bottom shows "Done" on the left and "Internet" on the right.

Figure B-27







# Appendix C

## Related Documents

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

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

