

# Troubleshooting

---

# 9

## Diagnosing and solving problems

This chapter provides information to help you diagnose and solve problems you might have with your wireless modem router. If you do not find the solution here, check the NETGEAR support site at <http://support.netgear.com> for product and contact information.

This chapter contains the following sections:

- *Router Not On*
- *No ISP Connection*
- *TCP/IP Network Not Responding*
- *Cannot Log in*
- *Changes Not Saved*
- *Firmware Needs to Be Reloaded*
- *Incorrect Date or Time*

## Router Not On

When you turn the power on, the power, LAN, wireless, DSL, and Internet LEDs should light as described here. If they do not, refer to the sections that follow for help.

1. When power is first applied, the Power LED lights.
2. After approximately 10 seconds, other LEDs light as follows:
  - a. The LAN ports LED lights when any local port is connected.
  - b. The 2.4 GHz and 5 GHz Wireless LEDs light.
  - c. The DSL LED lights when there is a link via the ADSL phone lines.
  - d. The Internet LED lights to indicate a connection to the ISP.

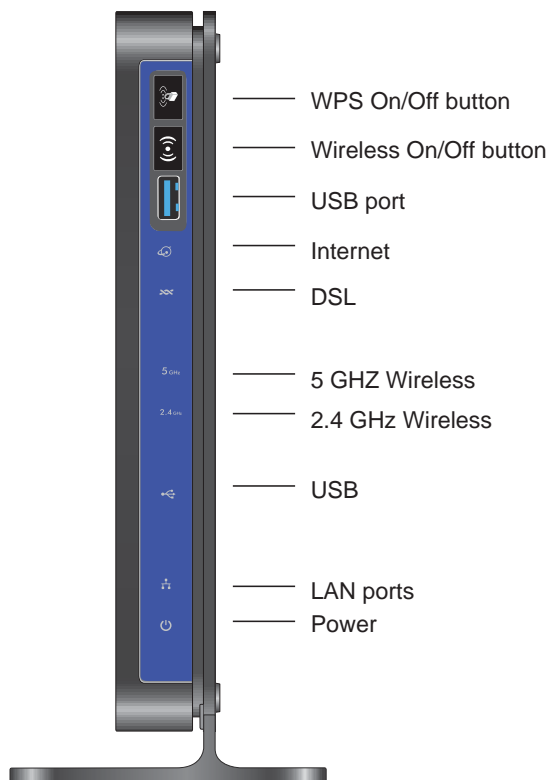


Figure 60. Front panel LEDs

## Power LED Is Off

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

- Check that the power cord is correctly connected to your router and the power supply adapter is correctly 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 could have a hardware problem and should contact NETGEAR Technical Support.

## Power LED Is Red

When the router is turned on, it performs a power-on self-test. If the Power LED turns red after a few seconds or at any other time during normal operation, there is a fault within the router.

If the Power LED turns red to indicate a router fault, turn the power off and on to see if the wireless modem router recovers. If the power LED is still red 1 minute after power-up:

- Turn the power off and on one more time to see if the wireless modem router recovers.
- Clear the router's configuration to factory defaults as explained in [Factory Settings](#) on page 154. This sets the router's IP address to 192.168.0.1.


If the error persists, you could have a hardware problem and should contact NETGEAR Technical Support.

## LAN LED Is Off

If the LAN LED does not light when the Ethernet connection is made, check the following:

- The Ethernet cable connections are secure at the wireless modem router and at the hub or workstation.
- The power is turned on to the connected hub or workstation.

## Wireless LEDs Are Off

If the 2.4 GHz and 5 GHz Wireless LEDs do not light, the radios may be turned off. Press the Wireless On/Off button on its front panel  to turn the radios back on.

## DSL or Internet LED Is Off

If the DSL or Internet LED does not light, check to make sure you are using the correct cable. When connecting the ADSL or Ethernet WAN port, use the cables that were supplied with the wireless modem router. If the DSL or Internet LED is still off, this could mean that there is no ADSL or Fiber/Cable modem service or the cable connected to the ADSL or Ethernet WAN port is bad.

See also [DSL LED Is Off](#) on page 146.

## No ISP Connection

If your router cannot access the Internet, first check the ADSL connection, and then check the WAN TCP/IP connections. See [Figure 4, Front panel LEDs](#) on page 14 for the location of the LEDs.

### ADSL Link

First determine whether you have a ADSL link with the service provider. The state of this connection is indicated by the DSL LED.

#### *DSL LED Is Green or Blinking Green*

You have a good ADSL connection. The service provider has connected your line correctly, and your wiring is correct.

#### *DSL LED Is Blinking Amber*

Your wireless modem router is attempting to make a ADSL connection with the service provider. The LED should turn green within several minutes.

If the DSL LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and use a microfilter on each telephone as described in [ADSL Microfilters](#) on page 18. If you connect the microfilters correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID), you might have poor-quality wiring in your house.

#### *DSL LED Is Off*

First disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and 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 DSL LED, check for 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 could be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The wireless modem router uses pins 2 and 3.

## Internet LED Is Red

If the Internet LED is red, the device could not connect to the Internet. Verify the following:

- Check that your log-in credentials are correct. See [Log In to the N600 Modem Router](#) on page 24 for more information.
- Check that the information you entered on the Basic Settings screen is correct. See [Manual Setup \(Basic Settings\)](#) on page 28.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the ADSL settings screen are correct.
- Find out if the ISP is having a problem. If it is, wait until that problem is cleared up and try again.

## Cannot Obtain an Internet IP Address

If your wireless modem router cannot access the Internet, and your Internet LED is green or blinking green, check whether the wireless modem router can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your wireless modem router must request an IP address from the ISP. You can determine whether the request was successful as follows:

1. Access the router menus at <http://192.168.0.1> and log in.
2. Under Maintenance, select **Router Status** and check that an IP address shows for the WAN port. If 0.0.0.0 shows, your wireless modem router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrect. See [Debug PPPoE or PPPoA](#) on page 148.
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account to the wireless modem router in the browser-based Setup Wizard. See [Setup Wizard](#) on page 27 for more information.
- Your ISP allows only one Ethernet MAC address to connect to the Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device and ask them to use the router's MAC address.
  - Configure your router to spoof your computer's MAC address through the Basic Settings screen. See [Manual Setup \(Basic Settings\)](#) on page 28.

## Debug PPPoE or PPPoA

Debug the PPPoE or PPPoA connection as follows:

1. Access the router menus at <http://192.168.0.1> and log in.
2. Under Maintenance, select **Router Status**.
3. Click the **Connection Status** button.
4. If all of the steps indicate OK, your PPPoE or PPPoA connection is working.
5. If any of the steps indicate Failed, you can attempt to reconnect by clicking **Connect**.

The wireless modem router continues to attempt to connect indefinitely. If you do not connect after several minutes, check that the service name, user name, and password you are using are correct. Also check with your ISP to be sure that there is no problem with their service.

---

**Note:** Unless you connect manually, the wireless modem router does not authenticate with PPPoE or PPPoA until data is transmitted to the network.

---

## Cannot Load an Internet Web Page

If your wireless modem router can obtain an IP address, but your browser cannot load any Internet Web pages:

- Your computer might not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the wireless modem router's configuration, reboot your computer, and verify the DNS address. Alternately, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the wireless modem router configured as its TCP/IP wireless modem router.

If your computer obtains its information from the wireless modem router by DHCP, reboot the computer, and verify the wireless modem router address.

## TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers have a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

## Test the LAN Path to Your Wireless Modem 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 task bar, 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 that the LAN port LED is on. If the LED is off, follow the instructions in [LAN LED Is Off](#) on page 145.
  - 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.

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

After you verify that the LAN path works correctly, test the path from your PC to a remote device. In the Windows Run screen, 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 described in [Test the LAN Path to Your Wireless Modem Router](#) on page 149 display. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default wireless modem router. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default wireless modem router.
- Check 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 ADSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single PC connected to that modem. In this case, configure your router to clone or spoof the MAC address from the authorized PC.

## Cannot Log in

If you cannot log in to the wireless modem router from a computer on your local network, check the following:

- The router is plugged in and it is on.
- You are using the correct login information. The login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.
- If you cannot connect wirelessly, try an Ethernet connection and view the router wireless settings and set up your wireless computer with corresponding wireless settings.
- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router. The LAN LED for the port you are using on the router should light up to show your connection.
- 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 192.168.0.2 to 192.168.0.254.
- If the computer IP address is 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address when the computer cannot reach a DHCP server. The



auto-generated addresses are in the range 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 as explained in *Factory Settings* on page 154. This sets the router's IP address to 192.168.0.1.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try closing the browser and relaunching it.

## Changes Not Saved

If the router does not save the changes you make in the router interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes might have occurred, but the old settings might be in the Web browser's cache.

## Firmware Needs to Be Reloaded

When you attempt to connect to the Internet, the browser might display a message similar to the one below telling you that you need to reload the router's firmware. This means a problem has been detected with the router's firmware.



**Figure 61. Reload firmware**

1. If you already have the firmware file on your PC, go directly to **step 2**. If you do not have the firmware file on your PC, obtain the firmware from the NETGEAR support site at <http://www.netgear.com/support> through another working Internet connection.
2. Click **Browse**.
3. Navigate to the firmware file.
4. Click **Upgrade**. A progress bar displays. The reload takes about 5 minutes to complete. When the firmware recovery is completed, the login screen displays so you can log in.

## Incorrect Date or Time

Select **Security > Schedule** to display the current date and time. The wireless modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000. This means the router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour. The router does not automatically sense daylight savings time. In the Schedule screen, select the **Adjust for Daylight Savings Time** check box.

# Supplemental Information

---




This appendix includes the factory default settings and technical specifications for the N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700, and instructions for wall-mounting the unit.

This appendix contains the following sections:

- *Factory Settings*
- *Technical Specifications*

## Factory Settings

You can return the wireless modem router to its factory settings. On the bottom of the wireless modem router, use the end of a paper clip or some other similar object to press and hold the Restore Factory Settings button  for at least 7 seconds. The wireless modem router resets, and returns to the factory settings. Your device will return to the factory configuration settings shown in the following table.

**Table 22. Factory Settings Description**

Feature	Default Behavior
<b>Router Login</b>	
User Login URL	http://www.routerlogin.net or http://www.routerlogin.com
User Name (case-sensitive)	admin
Login Password (case-sensitive)	password
<b>Internet Connection</b>	
WAN MAC Address	Use default address
WAN MTU Size	1492
Port Speed	AutoSense
<b>Local Network (LAN)</b>	
Lan IP	192.168.0.1
Subnet Mask	255.255.255.0
RIP Direction	None
RIP Version	Disabled
RIP Authentication	None
DHCP Server	Enabled
DHCP Starting IP Address	192.168.0.2
DHCP Ending IP Address	192.168.0.254
DMZ	Disabled
Time Zone	GMT
Time Zone Adjusted for Daylight Saving Time	Disabled
SNMP	Disabled

**Table 22. Factory Settings Description**

Feature		Default Behavior
<b>Firewall</b>		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
<b>Wireless</b>		
	Wireless Communication	Enabled
	Wi-Fi Network Name (SSID)	2.4 GHz Wireless Network: NETGEAR
		5 GHz Wireless Network: NETGEAR-5G
	Wireless security	Disabled
	Broadcast SSID	Enabled
	Transmission Speed	Auto <sup>1</sup>
	Country/Region	United States (in North America; otherwise, varies by region)
	RF Channel	Auto
	Operating Mode	Up to 145 Mbps
	Data Rate	Best
	Output Power	Full
	Access Point	Enabled
	Authentication Type	Pre-Shared Key
	Wireless Card Access List	All wireless stations allowed

*1. Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.*

## Technical Specifications

**Table 23. Technical Specifications Description**

<b>Network Protocol and Standards Compatibility</b>	
Data and routing protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
<b>Power Adapter</b>	
North America	120V, 60 Hz, input
UK, Australia	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
All regions (output)	12 V AC @ 2.5A output
<b>Physical</b>	
Dimensions	6.80 in. x 5.03 in. x 1.28 in. 172.7 mm x 127.7 mm x 32.5 mm
Weight	0.61 lbs. 0.275 kg
<b>Environmental</b>	
Operating temperature	0° to 40° C (32° to 104° F)
Operating humidity	10% to 90% relative humidity, noncondensing
Storage temperature	-20° to 70° C (-4° to 158° F)
Storage humidity	5 to 95% relative humidity, noncondensing
<b>Regulatory Compliance</b>	
Meets requirements of	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
<b>Interface Specifications</b>	
LAN	10BASE-T or 100BASE-Tx, RJ-45
WAN	ADSL, Dual RJ-11, pins 2 and 3 T1.413, G.DMT

# NETGEAR VPN Configuration

# B

## Case study on how to set up a VPN

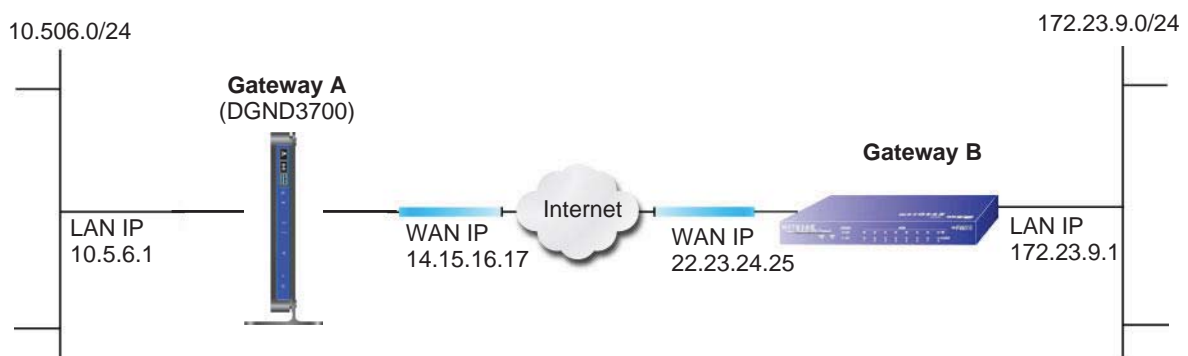
This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DGND3700 to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>).

## Configuration Profile

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

**Table 24. Wireless Modem Router to Gateway B Profile Summary**

VPN Consortium Scenario	Scenario 1 (Identity Using Preshared Secrets)
Type of VPN	LAN-to-LAN or gateway-to-gateway (not PC/client-to-gateway)
Security scheme:	IKE with pre-shared secret/key (not certificate based)
IP addressing:	
NETGEAR-Gateway A	Static IP address
NETGEAR-Gateway B	Static IP address



**Figure 62. VPNC Example, Network Interface Addressing**

## Step-by-Step Configuration

1. Use the VPN Wizard to configure Gateway A (DGND3700) for a gateway-to-gateway tunnel (see [Setting Up a Gateway-to-Gateway VPN Configuration](#) on page 99), 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
DGND3700	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. For the connection name, enter **toGW\_B**.
  - b. For the remote WAN's IP address, enter **22.23.24.25**.
  - c. Enter the following:
    - IP Address. **172.23.9.1**
    - Subnet Mask. **255.255.255.0**
  - d. In the Summary screen, click **Done**.
2. Use the VPN Wizard to configure the Gateway B for a gateway-to-gateway tunnel (see [Setting Up a Gateway-to-Gateway VPN Configuration](#) on page 99), being certain to use appropriate network addresses for the environment.
    - a. For the connection name, enter **toGW\_A**.
    - b. For the remote WAN's IP address, enter **14.15.16.17**.
    - c. Enter the following:
      - IP Address. **10.5.6.1**
      - Subnet Mask. **255.255.255.0**
    - d. In the Summary screen, click **Done**.

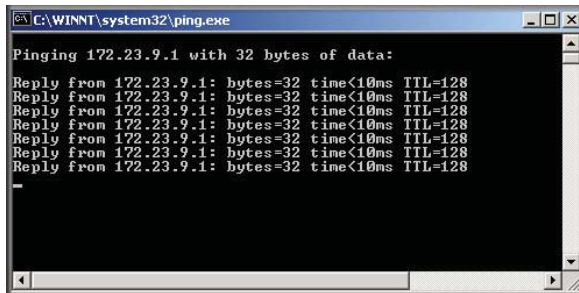


3. On the Gateway B router menu, under VPN, select **IKE Policies**, and click the **Edit** button to display the IKE Policy Configuration screen:

4. On Gateway B router menu, under VPN, select **VPN Policies**, and click the **Edit** button to display the VPN - Auto Policy screen:

5. Test the VPN tunnel by pinging the remote network from a PC attached to Gateway A (wireless modem router).
  - a. Open the command prompt (select **Start > Run > cmd**).

b. Type ping 172.23.9.



If the pings fail the first time, try the pings a second time.

## Wireless Modem Router with FQDN to Gateway B

This section is a case study on how to configure a VPN tunnel from a NETGEAR wireless modem router to a gateway using a fully qualified domain name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (found at <http://www.vpnc.org/InteropProfiles/Interop-01.html>).

### Configuration Profile

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

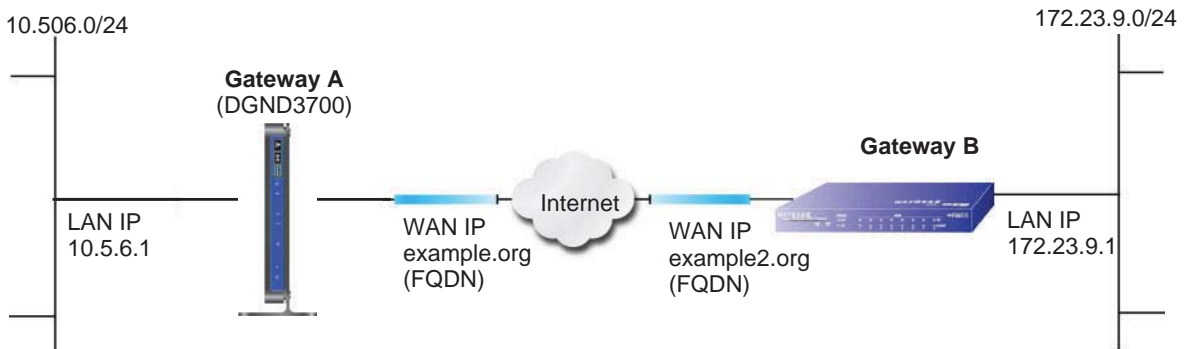


Figure 63. VPNC Example, Network Interface Addressing

Table 25. Wireless Modem Router with FQDN to Gateway B 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 pre-shared secret/key (not certificate based)
IP addressing:	

**Table 25. Wireless Modem Router with FQDN to Gateway B Profile Summary**

VPN Consortium Scenario		Scenario 1
	NETGEAR-Gateway A	Fully qualified domain name (FQDN)
	NETGEAR-Gateway B	FQDN

### Using a Fully Qualified Domain Name (FQDN)

Many ISPs 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 third-party service instead of a permanent and unchanging IP address to establish bidirectional VPN connectivity.

To use DDNS, you must register with a DDNS service provider. Some 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 a sample FQDN provided by a DDNS service provider. In this case we established the hostname `dgnd3300v2.dyndns.org` for Gateway A using the DynDNS service. Gateway B uses the DDNS service provider when establishing a VPN tunnel.

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

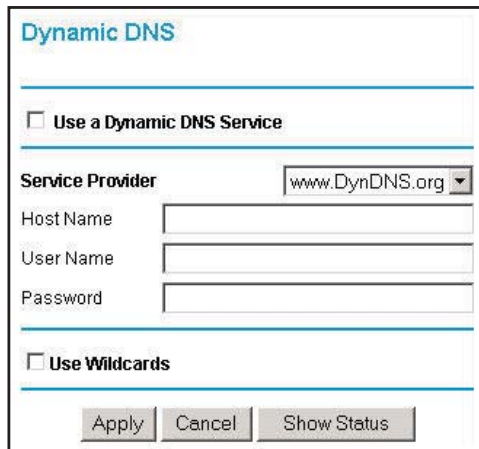
## Step-by-Step Configuration

1. Log in to Gateway A (your wireless modem router) as described in [Log In to the N600 Modem Router](#) on page 24.

This example assumes that you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. On Gateway A, configure the Dynamic DNS settings.

- a. Under Advanced, select **Dynamic DNS**.

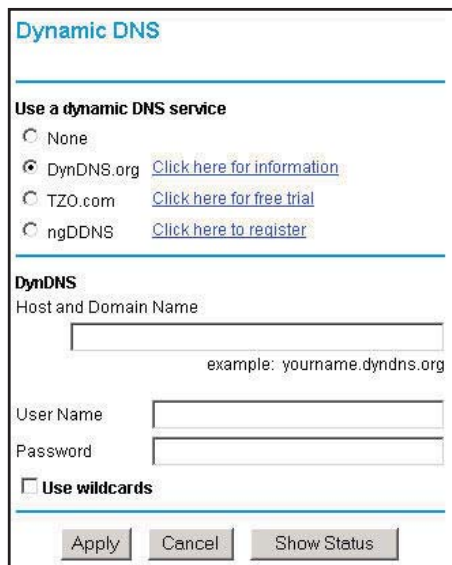


- b. Fill in the fields with account and host name settings.
- Select the **Use a Dynamic DNS Service** check box.
  - In the Host Name field, type **dgnd3300v2.dyndns.org**.
  - In the User Name field, enter the account user name.
  - In the Password field, enter the account password.
- c. Click **Apply**.
- d. Click **Show Status**. The resulting screen should show Update OK: good:



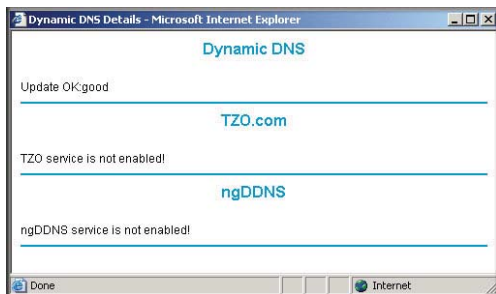
3. On NETGEAR Gateway B, configure the Dynamic DNS settings. Assume a correctly configured DynDNS account.
- a. From the main menu, select **Dynamic DNS**.
- b. Select the **DynDNS.org** radio button.

The Dynamic DNS screen displays:



- c. Fill in the fields with the account and host name settings.
  - In the Host and Domain Name field, enter **fvl328.dyndns.org**.
  - In the User Name field, enter the account user name.
  - In the Password field, enter the account password.
- d. Click **Apply**.
- e. Click **Show Status**.

The resulting screen should show Update OK: good:

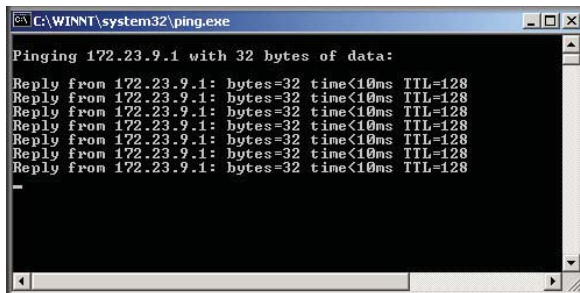


- 4. Configure the N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700 as in the gateway-to-gateway procedures using the VPN Wizard (see [Setting Up a Gateway-to-Gateway VPN Configuration](#) on page 99), being certain to use appropriate network addresses for the environment.

The LAN addresses used in this example are as follows:

Device	LAN IP Address	LAN Subnet Mask
DGND3700	10.5.6.1	255.255.255.0
FVL328	172.23.6.1	255.255.255.0

- a. For the connection name, enter **toFVL328**.
  - b. For the remote WAN's IP address, enter **fv1328.dyndns.org**.
  - c. Enter the following:
    - IP Address. **172.23.9.1**
    - Subnet Mask. **255.255.255.0**
5. Configure the **FVL328** as in the gateway-to-gateway procedures for the VPN Wizard (see [Setting Up a Gateway-to-Gateway VPN Configuration](#) on page 99), being certain to use appropriate network addresses for the environment.
- a. For the connection name, enter **toDGND3300v2**.
  - b. For the remote WAN's IP address, enter **dgnd3300v2.dyndns.org**.
  - c. Enter the following:
    - IP Address. **10.5.6.1**
    - Subnet Mask. **255.255.255.0**
6. Test the VPN tunnel by pinging the remote network from a PC attached to the N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700.
- a. Open the command prompt (select **Start > Run > cmd**)
  - b. Type `ping 172.23.9.1`.



If the pings fail the first time, try the pings a second time.

## Configuration Summary (Telecommuter Example)

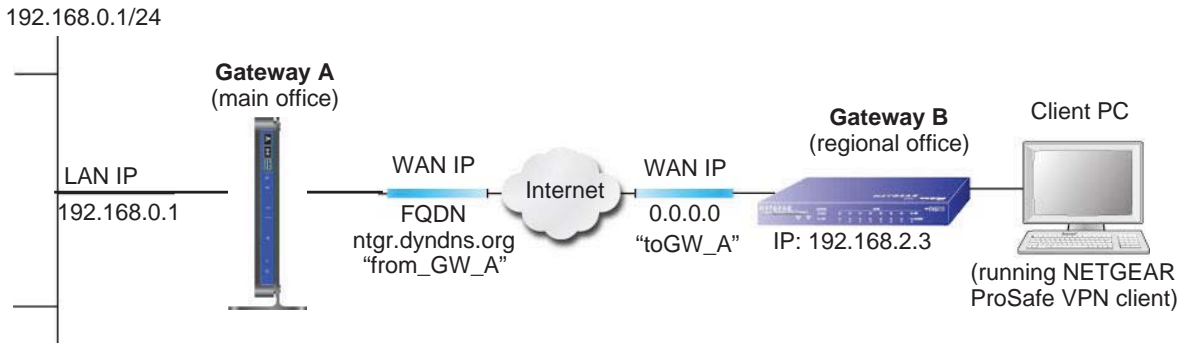
The configuration in this section follows the addressing and configuration mechanics defined by the VPN Consortium. Gather the necessary information before you begin configuration. Verify that the firmware is up to date, and make sure you have all the addresses and parameters to be set on both sides.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

**Table 26. Configuration Summary (Telecommuter Example)**

VPN Consortium Scenario	Scenario 1
Type of VPN:	PC/client-to-gateway, with client behind NAT router
Security scheme:	IKE with pre-shared secret/key (not certificate based)
IP addressing:	

**Table 26. Configuration Summary (Telecommuter Example)**

VPN Consortium Scenario	Scenario 1
Gateway	Fully qualified domain name (FQDN)
Client	Dynamic



**Figure 64. Telecommuter Example**

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

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN client and a network gateway involves two steps, described in the following sections:

- *Step 1: Configure Gateway A (VPN Router at Main Office)* on page 166.
- *Step 2: Configure Gateway B (VPN Router at Regional Office)* on page 167 describes configuring the NETGEAR ProSafe VPN client endpoint.

## Step 1: Configure Gateway A (VPN Router at Main Office)

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

**VPN - Auto Policy**

**General**  
 Policy Name: fromGW\_A  
 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: fromGW\_A.com  
 Remote Identity Type: Fully Qualified Domain Name  
 Data: toGW\_A.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

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

**VPN Policies**

#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	GtoG	auto	192.168.0.1/255.255.255.0	192.168.10.1/255.255.255.0	3des

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

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



## Step 2: Configure Gateway B (VPN Router at Regional Office)

This procedure assumes that the PC running the client has a dynamically assigned IP address.

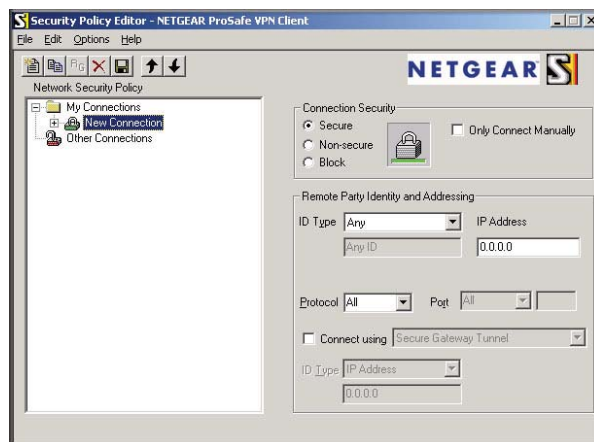
The PC must have a VPN client program installed that supports IPsec (in this case study, the NETGEAR VPN ProSafe Client is used). Go to the NETGEAR website ([www.netgear.com](http://www.netgear.com)) for information about how to purchase the NETGEAR ProSafe VPN Client.

---

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

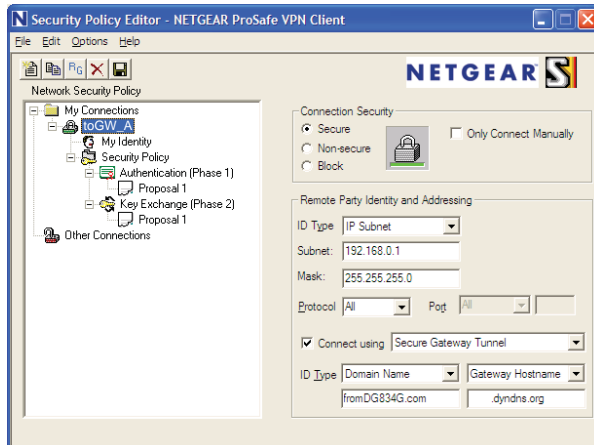
---

1. Install the NETGEAR ProSafe VPN Client on the remote PC, and then reboot.
  - a. You might need to insert your Windows CD to complete the installation.
  - b. If you do not have a modem or dial-up adapter installed in your PC, you might see the warning message stating “The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed.” You can disregard this message.
  - c. Install the IPsec component. You might have the option to install either the VPN adapter or the IPsec component or both. The VPN adapter is not necessary.
  - d. The system should show the ProSafe icon (🔒) in the system tray after you reboot.
  - 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, select **Add > Connection**. A New Connection listing appears in the list of policies.
  - c. Rename the new connection to match the connection name you entered in the VPN settings of Gateway A. Choose connection names that make sense to the people using and administrating the VPN.



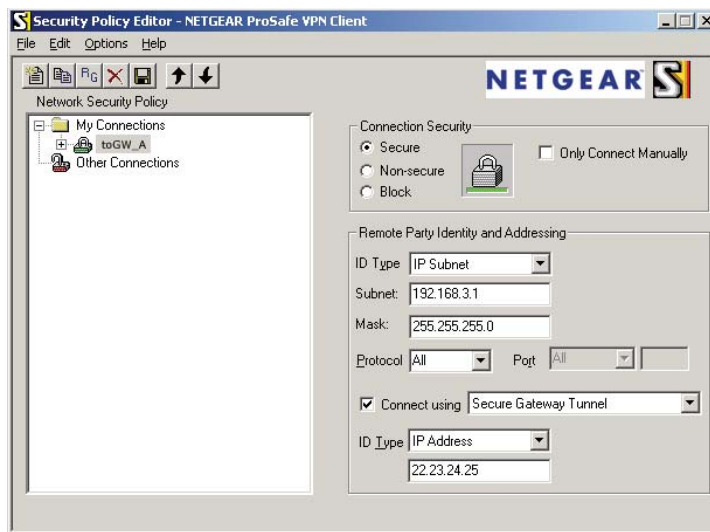
**Note:** In this example, the connection name on the client side of the VPN tunnel is toGW\_A. It does not have to match the VPN\_client connection name used on the gateway side of the VPN tunnel because connection names do not affect how the VPN tunnel functions.

- d. In the Connection Security section, select **Secure**.



- e. In the ID Type drop-down list, select **IP Subnet**.
  - f. In this example, in the Subnet field, type **192.168.0.1** as the network address of the wireless modem router.
  - g. In the Mask field, enter **255.255.255.0** as the LAN subnet mask of the wireless modem router.
  - h. In the Protocol drop-down list, select **All** to allow all traffic through the VPN tunnel.
  - i. Select the **Connect using Secure Gateway Tunnel** check box.
  - j. In the ID Type drop-down list, select **Domain Name**, and enter **fromGW\_A.com** (in this example).
  - k. Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).
3. Configure the security policy in the wireless modem router software.
    - a. In the Network Security Policy list, expand the new connection by double-clicking its name or clicking the + symbol. My Identity and Security Policy appear below the connection name.

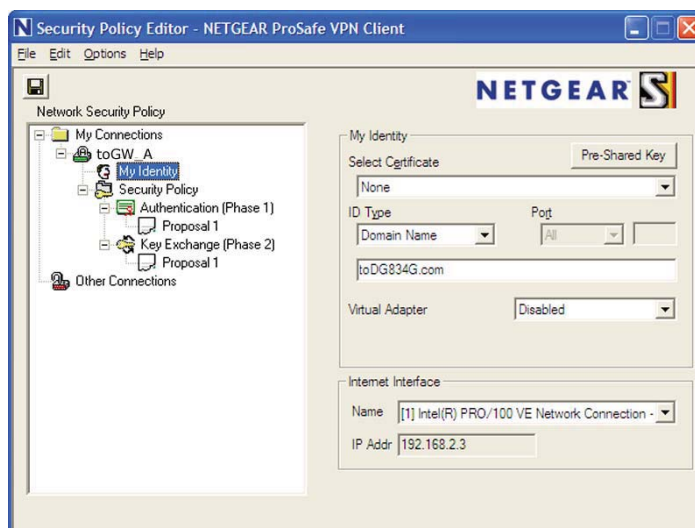
- b. Click **Security Policy** to show the Security Policy screen.



- c. In the Select Phase 1 Negotiation Mode group, select the **Main Mode** radio button.
4. Configure the VPN client identity.

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



- b. In the Select Certificate list, select **None**.
- c. In the ID Type list, select **Domain Name**, and enter **toGW\_A.com** (in this example).
- d. In the Virtual Adapter list, select **Disabled**.

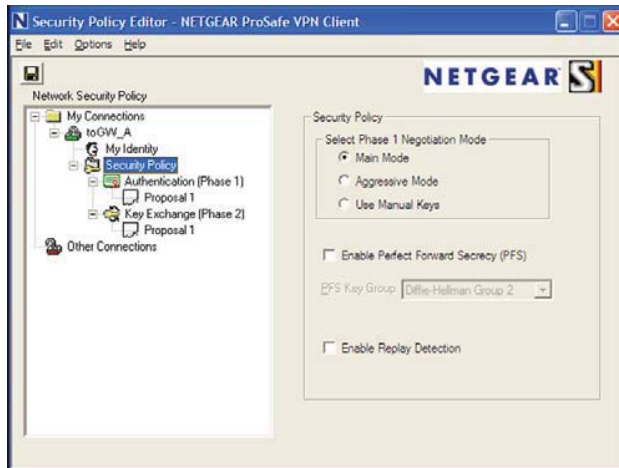
- e. In the Internet Interface section, select **Intel PRO/100VE Network Connection** (in this example; your Ethernet adapter might be different) in the Name list, and then in the IP Addr list, enter **192.168.2.3** (in this example).
- f. Click the **Pre-Shared Key** button.
- g. In the Pre-Shared Key screen, click **Enter Key**. Enter the N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700's pre-shared key and click **OK**. In this example, 12345678 is entered, though the screen shows asterisks. This field is case-sensitive.



5. Configure the VPN Client Authentication Proposal.

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

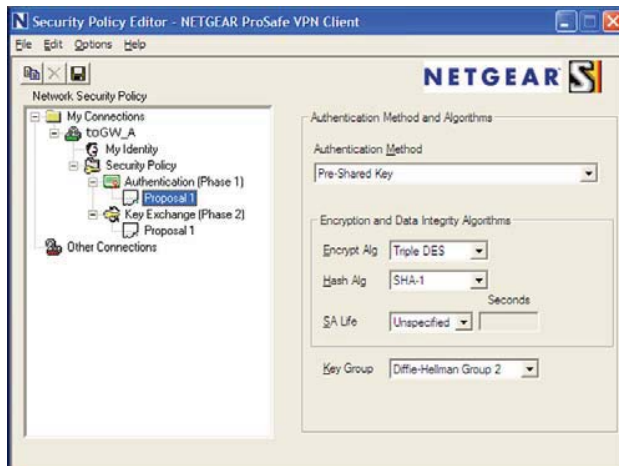
- a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double-clicking its name or clicking the + symbol.
- b. Expand the Authentication subheading by double-clicking its name or clicking the + symbol. Then select **Proposal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



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

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

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



- b. In the SA Life drop-down list, select **Unspecified**.
  - c. In the Compression drop-down list, select **None**.
  - d. Select the **Encapsulation Protocol (ESP)** check box.
  - e. In the Encrypt Alg drop-down list, select the type of encryption. In this example, use **Triple DES**.
  - f. In the Hash Alg drop-down list, select **SHA-1**.
  - g. In the Encapsulation drop-down list, select **Tunnel**.
  - h. Leave the **Authentication Protocol (AH)** check box cleared.
7. Save the VPN client settings.

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

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

8. Check the VPN connection.

To check the VPN connection, you can initiate a request from the remote PC to the VPN router's network by using the Connect option in the wireless modem router screen:

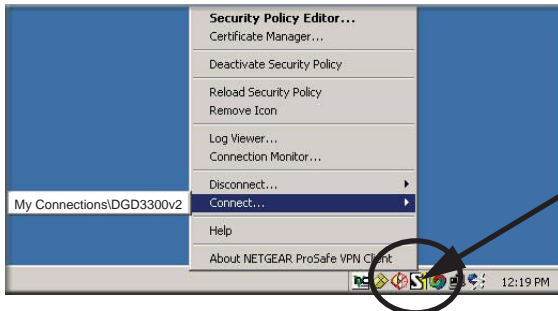


Right-click the system tray icon to open the pop-up menu.

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 pop-up menu.
- b. Select **Connect** to open the My Connections list.
- c. Select **toDGND3300v2**.

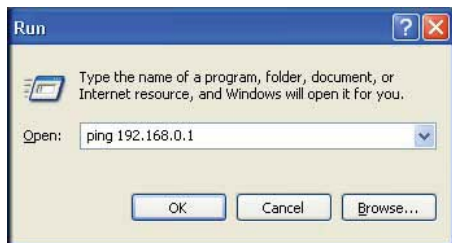
The wireless modem router reports the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.



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

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

- a. Establish an Internet connection from the PC.
- b. On the Windows taskbar, click the **Start** button, and then select **Run**.
- c. Type `ping -t 192.168.0.1`, and then click **OK**.



This causes a continuous ping to be sent to the VPN router. Within 2 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
```

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

---

**Note:** You can use the VPN router diagnostics to test the VPN connection from the VPN router to the client PC. To do this, select **Diagnostics** on the wireless modem router main menu.

---

## Monitoring the VPN Tunnel (Telecommuter Example)

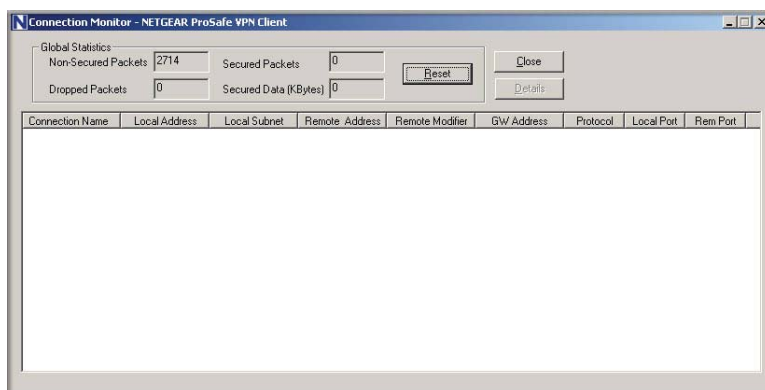
To view information about the progress and status of the VPN client connection, open the Log Viewer. In Windows, click **Start**, and select **Programs > N600 Wireless Dual Band Gigabit ADSL2+ Modem Router DGND3700 > Log Viewer**.

---

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

---

The Connection Monitor screen displays:



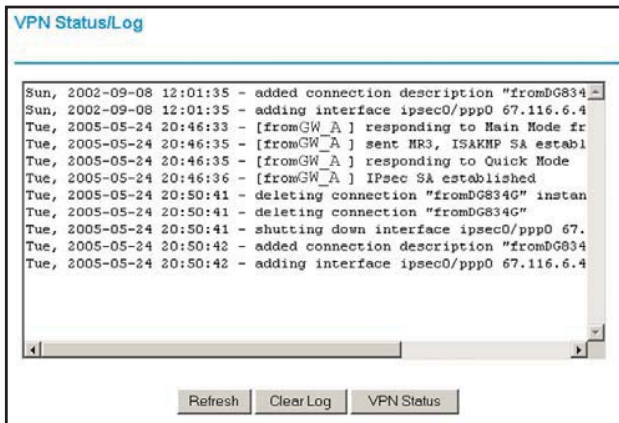
While the connection is being established, the connection name listed in this screen shows SA before the name of the connection. When the connection is successful, the SA changes to the yellow key symbol.

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

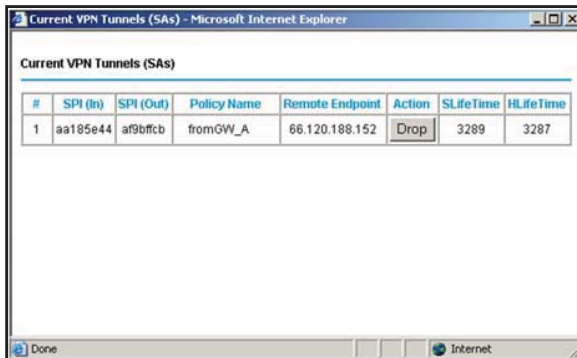
## Viewing the VPN Router’s VPN Status and Log Information

To view information about the status of the VPN client connection, open the VPN router’s VPN Status screen:

1. On the wireless modem router main menu, select **Router Status**, and then click the **VPN Status** button. The VPN Status/Log screen displays:



2. To view the VPN tunnels status, click **VPN Status**.





# Notification of Compliance



## NETGEAR Wireless Routers, Gateways, APs

### Regulatory Compliance Information

Placeholder for dual-band compliance appendix.

### Interference Reduction Table

The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

**Table 27. Interference Reduction Table**

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

# Index

## A

- AC power adapter input **14**
- access lists **43**
- accessing remote computer **49**
- adapter, wireless **23**
- adding
  - custom service **53**
- addresses, DNS **30**
- ADSL
  - see also DSL
  - statistics, viewing **69**
- ADSL microfilter
  - filter, described **18**
- ADSL microfilters **18**
- ADSL settings **32**
- ADSLport **13**
- Advanced Wireless Settings screen **128**
- alerts, emailing **59**
- Application Level Gateway (ALG), disabling **123**
- approved USB devices **80**
- attached devices, viewing **71**
- authentication proposal **95, 96**
- Auto Policy to configure VPN tunnels **110**
- automatic firmware checking **64**
- automatic Internet connection **28**

## B

- back panel **13**
- backing up configuration **66**
- Basic Settings screen
  - described **29**
  - manual setup **28**
- blocking content and services **47**
- blocking keywords, examples **48**
- blocking settings examples **48**
- box contents **11**
- bridged networks **130**

## C

- changes not saved, router **151**

- client-to-gateway VPN tunnels **85**
- compliance **175**
- configuration file
  - backing up **66**
  - erase **66**
  - managing **66**
  - restoring **66**
- configuration, wireless network **41**
- configuring
  - port forwarding **53**
  - port triggering **55**
  - security policy **94**
  - VPN tunnels **86, 88, 99, 160**
- connecting USB drive **81**
- connecting wirelessly **17**
- content filtering **47**
- custom service (port forwarding) **53**

## D

- date and time **152**
- daylight savings time **58, 152**
- deactivating VPN tunnels **107, 108**
- default demilitarized zone (DMZ) server **122**
- default factory settings, see factory settings
- deleting
  - VPN tunnels **109**
- denial of service (DoS)
  - port scans **121**
  - protection **47**
- devices, adding **39**
- diagnostic utilities **71**
- disable SSID **37**
- disabling
  - firewalls **31**
  - SIP ALG **123**
  - SSID broadcast **37**
- disconnecting USB drive **80**
- DNS servers **49**
- Domain Name Server (DNS) addresses **30, 123**
- Domain Name Server (DNS), secondary **30**
- DSL port LED **15**
- DSL settings **31**

Dynamic DNS [123](#)

Dynamic Host Configuration Protocol (DHCP) server [125](#)

## E

email notices [59](#)

encryption algorithm [96](#)

encryption keys [38](#)

erasing configuration file [66](#)

## F

factory settings

list of [154](#)

resetting [12](#)

file and printer sharing [82](#)

file sharing [73](#)

filtering content [47](#)

firmware

automatic check [64](#)

reload firmware message [151](#)

upgrade [64](#), [136](#)

upgrade at log in [25](#)

upgrade manually [65](#)

front panel [14](#)

front panel LEDs [14](#)

FTP, sharing files using [75](#)

fully qualified domain name (FQDN), configuring VPN tunnels using [160](#)

## G

gateway IP address [30](#)

gateway-to-gateway VPN tunnels [86](#), [99](#)

guest devices, adding [39](#)

## H

host name [29](#)

host trusted [48](#)

## I

IKE protocol [110](#)

installing

manual setup [28](#)

Internet port [28](#)

Internet port LEDs [15](#)

Internet port, no connection [32](#)

Internet Relay Chat (IRC) [50](#)

Internet Service Provider (ISP), see ISP

Internet traffic statistics [142](#)

IP address [81](#)

DHCP [23](#)

LAN service [124](#)

reserved [125](#)

IP setup, LAN [124](#)

ISP

account information [23](#)

Basic Settings screen [29](#)

DSL settings [31](#)

DSL synchronization [15](#)

ISP login [24](#)

## K

keep-alive, IKE [111](#)

keywords

blocking [48](#)

deleting [48](#)

## L

LAN

setup [124](#)

LAN port LEDs [16](#)

LAN ports [13](#)

LAN setup [124](#)

large files, sharing [75](#)

LEDs

troubleshooting [144](#)

verifying cabling [20](#)

local servers, port forwarding to [53](#)

Log Viewer [98](#)

logging in

cannot [150](#)

changing password [32](#), [63](#)

ISP [24](#)

router [24](#)

time-out [33](#)

types [33](#)

upgrade firmware [25](#)

login time-out [32](#), [63](#)

logs, emailing [59](#)

## M

MAC addresses

configuring [31](#)

described [37](#)

filtering by [44](#)

rejected [150](#)

restricting access by [43](#), [45](#)

spoofing [147](#)

maintenance settings **63**  
 manual logout **33**  
 manual setup **28**  
 manual setup, Basic Settings screen **28**  
 manually configuring VPN policies **117**  
 Maximum Transmit Unit (MTU) **122**  
 MD5 authentication **112**  
 menus, described **26**  
 metric, number of routers **138**  
 mixed mode security options **38**  
 multi-point bridge mode **132**

## N

NAT (Network Address Translation) **49**  
 NETGEAR ProSafe VPN Client **92**  
 Network Address Translation (NAT) **31**  
 network folder  
     creating **79**  
     editing **77**  
 Network Time Protocol (NTP) **58, 152**  
 network troubleshooting **148**  
 no Internet connection **32**

## O

On/Off button **14**  
 On/Off LED **17**  
 one-line ADSL microfilter **18**  
 online help, router **26**

## P

passphrases **46**  
     changing **45**  
     WPA-802.1x **45**  
 passwords, see passphrases  
 ping **98, 172**  
 pinging WAN port **122**  
 Plug and Play, Universal (UPnP) **139**  
 plug and play, universal (UPnP) **139**  
 point-to-point bridge mode **131**  
 Point-to-Point Tunneling Protocol (PPTP) **28**  
 port forwarding **51, 52, 53**  
     configuring **53**  
     example **51**  
 port numbers **57**  
 port scanning, disabling **121**  
 port triggering **50, 52, 55**  
     configuring **55**  
     example **50**

ports  
     listed, back panel **13**  
 positioning the router **17**  
 power adapter, AC **14**  
 preset security  
     passphrase **36, 45**  
     security option **36**  
     SSID **36**  
 pre-shared key **38**  
 primary DNS addresses **30**  
 Push 'N' Connect, see WPS

## Q

Quality of Service (QoS) **126, 127**

## R

RADIUS server **38**  
 range of wireless connections **17**  
 remote management **81, 135**  
 removing USB drive **80**  
 repeater mode with wireless client association **134**  
 replace existing router **23**  
 reserved IP address **125**  
 restore  
     configuration file **66**  
     factory settings button **154**  
 restricting wireless access by MAC addresses **45**  
 router interface, described **26**  
 router, status **67**  
 Routing Information Protocol (RIP) **124**

## S

secondary DNS **30**  
 Secure Sockets Layer (SSL) **35**  
 security **37**  
     see also security options  
 security association (SA) **87**  
 security features **36**  
 security options  
     described **37**  
     settings **37**  
 security PIN **12, 40**  
 security policy, configuring **94**  
 security settings **47**  
 sending logs by email **59**  
 services **57**  
 Session Initiation Protocol (SIP), disabling **123**  
 setting time zone **58**

Setup Wizard **28**  
SHA-1 authentication **112**  
sharing files **73**  
Simple Mail Transfer Protocol (SMTP) **60**  
sites, blocking **48**  
SSID  
    described **43**  
    disable **37**  
static routes **137, 138**  
statistics, viewing **69**  
status  
    Internet connection **70**  
    router **67**  
storage drive. See USB storage

## T

TCP/IP  
    network troubleshooting **148**  
    no Internet connection **32**  
technical specifications **156**  
technical support **2**  
Temporal Key Integrity Protocol (TKIP) **38**  
time of day **152**  
time zone, setting **58**  
time-out  
    port triggering **56**  
time-stamping **58**  
trademarks **2**  
traffic metering **141, 142**  
troubleshooting **143**  
    cannot log in **150**  
    date or time incorrect **152**  
    firmware reload **151**  
    LEDs **144, 145**  
    network **148**  
    router changes not saved **151**  
    router not on **144**  
trusted host **48**  
Trusted IP Address field **48**  
trusted wireless stations **44**  
turn off wireless connectivity **37, 145**  
two-line ADSL microfilter **19**

## U

Universal Plug and Play (UPnP) **139**  
unmounting USB drive **80**  
upgrading firmware **64, 136**  
USB devices, approved **80**  
USB drive requirements **73**

USB drive, unmounting **80**  
USB port **15**  
USB port LED **16**  
USB storage **72**  
    advanced **78, 140**  
    basic settings **75**  
    connecting **81**  
    creating a network folder **79**  
    editing a network folder **77**  
    file sharing scenarios **73**

## V

Virtual Channel Identifier (VCI) **24, 31**  
Virtual Path Identifier (VPI) **24, 31**  
VPN Auto Policy **110, 114, 115**  
VPN client **92**  
VPN Log Viewer **98, 173**  
VPN Manual Policy **117**  
VPN network connections **110**  
VPN tunnels  
    activating **103, 105**  
    client-to-gateway **85**  
    configuring **160**  
    control **103**  
    deactivating **107, 108**  
    deleting **109**  
    gateway-to-gateway **86, 99**  
    monitoring **173**  
    special setup **109**  
    status **106**  
VPN Wizard **101, 102**  
VPNs **85, 86**  
    overview **85**  
    pinging **172**  
    planning **86**  
    status **103, 174**

## W

WAN **121**  
    advanced setup **121**  
    ping response **122**  
    settings **121, 122**  
WAN port  
    scanning **121**  
Wi-Fi Protected Setup (WPS) **39, 40**  
    adding devices **39**  
    keep existing settings **129**  
    settings **128**  
Wi-Fi-certified products **39**  
Wired Equivalent Privacy (WEP) encryption **46**  
    passphrase **46**  
    when to use **38**

- wireless access points **43**
- wireless adapter **23**
- wireless advanced settings **128**
- wireless bridging and repeating **130**
- wireless channel **43**
- wireless connections **17**
- wireless connectivity **37, 145**
- wireless distribution system (WDS) **130, 131, 132, 134**
- wireless isolation **43**
- Wireless LAN (WLAN) **69**
- wireless LED **15, 16**
- wireless mode **43**
- wireless network configuration **41**
- wireless network settings **43**
- wireless region **43**
- wireless security **36**
- wireless security options **37**
- Wireless Settings screen **41**
- wireless settings, SSID broadcast **43**
- Wireless Stations Access List **43**
- WPA encryption **38**
- WPA2 encryption **38**
- WPA2-PSK encryption **38**
- WPA-802.1x encryption **38**
  - passphrases **45**
  - RADIUS servers **38**
- WPA-PSK encryption **38**
- WPA-PSK/WPA2-PSK mixed mode **38**
- WPS button **40**
- WPS LED **14**
- WPS, see Wi-Fi Protected Setup (WPS)
- WPS-capable devices **39**
- WPS-PSK encryption **38**
- WPS-PSK+ WPA2-PSK encryption **38**
- wrong date or time **152**