NETGEAR

# N300 Wireless ADSL2+ Modem Router DGN2200

## User Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

February 2011
202-10563-04
v1.0

## Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

## Trademarks



## Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

# Contents

## Chapter 4 Content Filtering Settings



## Chapter 5 Network Maintenance

## Chapter 6 USB Storage



## Chapter 7 Advanced Settings



## Chapter 8 Virtual Private Networking

## Chapter 9 Troubleshooting



## Appendix A Supplemental Information



## Appendix B NETGEAR VPN Configuration

# Hardware Setup

# 1

## Getting to know your modem router

The N300 Wireless ADSL2+ Modem Router DGN2200 provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). It has a built-in DSL modem, is compatible with all major DSL Internet service providers, lets you block unsafe Internet content and applications, and protects the devices (PCs, gaming consoles, and so on) that you connect to your home network.

For more information on the topics covered in this manual, visit the Support website at *http://support.netgear.com*.

If you have not already set up your new modem router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 2, Modem Router Setup*, explains how to set up your Internet connection.

This chapter contains the following sections:

# Unpack Your Modem Router

Your box should contain the following items:

- N300 Wireless ADSL2+ Modem Router DGN2200
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Microfilters and splitters (quantity and type vary by region)
- *Resource CD* with NETGEAR Genie setup
- Installation guide with cabling and modem router setup instructions

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

# Hardware Features

Before you cable your modem router, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

## Label

The label on the bottom of the modem router shows the Restore Factory Settings button, security PIN, preset login information, MAC address, and serial number.

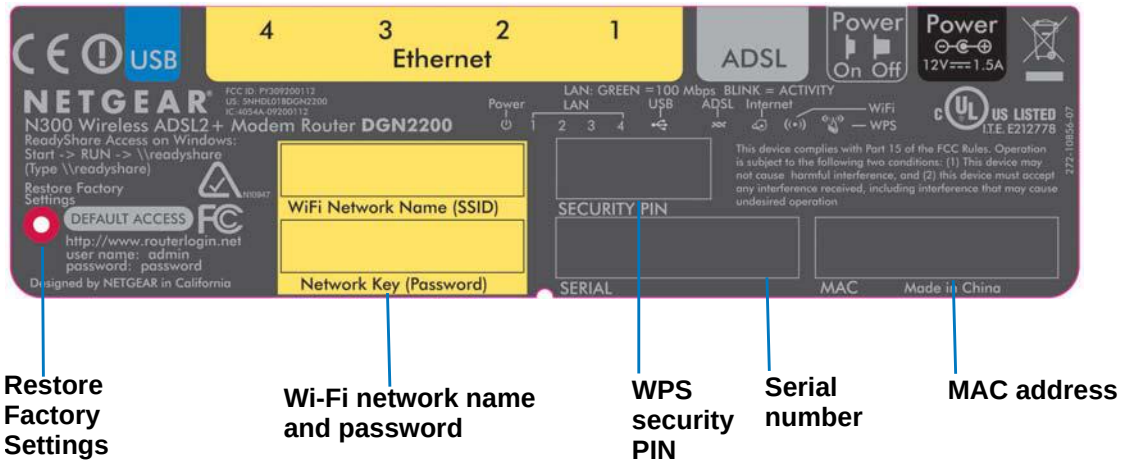



**Figure 1. Label on modem router bottom**

See *Preset Security* on page 30 for information about preset security and MAC addresses.
See *Factory Settings* on page 138 for information about restoring factory settings.

## Back Panel

The back panel has the On/Off button and port connections as shown in the figure.

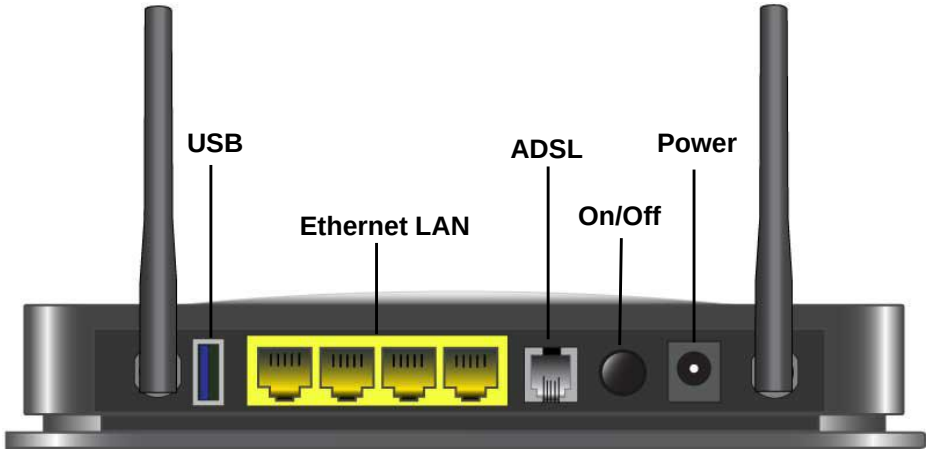



**Figure 2. Back panel port connections**

## Front Panel

The modem router front panel has the status LEDs and icons shown in the figure. Note that the Wireless and WPS icons are buttons.

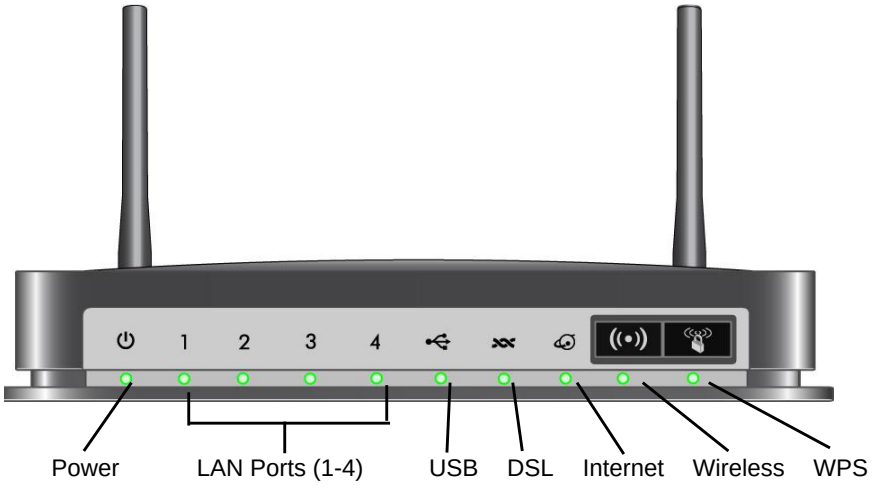



**Figure 3. Front panel LEDs and icons**

The following table describes the LEDs, icons, and buttons on the front panel from left to right.

**Table 1. Front Panel LEDs**

| Icon | LED Activity | Description |
|---|---|---|
| Power  | Solid green | Power is supplied to the modem router. |
| | Solid red | POST (power-on self-test) failure or a device malfunction has occurred. |
| | Off | Power is not supplied to the modem router. |
| | Restore factory settings | The LED blinks momentarily when the Restore Factory Settings button on the bottom of the unit is pressed for 6 seconds. The Power LED then blinks red three times when the Restore Factory Settings button is released and then turns green as the gateway resets to the factory defaults. |
| LAN  | Solid green | The LAN port has detected an Ethernet link with a device. |
| | Blinking green | Data is being transmitted or received. |
| | Off | No link is detected on this port. |
| USB  | Off | • No USB device connected.<br>• “Safely Remove Hardware” has been activated.<br>• An error has occurred with the device. |
| | Solid green | USB device is ready to use. |
| | Blinking green | USB device is in use. |
| DSL  | Solid green | You have a DSL connection. In technical terms, the DSL port is synchronized with an ISP’s network-access device. |
| | Blinking green | Indicates that the modem router is negotiating the best possible speed on the DSL line. |
| | Off | The unit is off or there is no IP connection. |
| Internet  | Solid green | You have an Internet connection. If this connection is dropped due to an idle time-out but the DSL connection is still present, the light stays green. If the Internet connection is dropped for any other reason, the light turns off. |
| | Solid red | The Internet (IP) connection failed. See *Troubleshooting the Internet Connection* on page 131 for troubleshooting information. |
| | Blinking green | Data is being transmitted over the DSL port. |
| Wireless  Icon is on the Wireless button | Off | No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection). |
| | Solid green | There is wireless connectivity. |
| | Blinking green | Data is being transmitted or received over the wireless link. |
| | Off | There is no wireless connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity. See *Turn Off Wireless Connectivity* on page 30 for more information about the use of this button. |
| WPS  Icon is on the WPS button | Solid green | Indicates that wireless security has been enabled. |
| | Blinking green | WPS-capable device is connecting to the device. |
| | Off | WPS is not enabled. See *Wi-Fi Protected Setup (WPS) Method* on page 32 for more information about the use of this button. |

## Modem Router Stand

For optimal wireless network performance, use the stand (included in the package) to position your modem router upright.

1. Orient your modem router vertically.
2. Insert the tabs of the stand into the slots on the bottom of your modem router as shown.
3. Place your modem router in a suitable area for installation (near an AC power outlet and accessible to the Ethernet cables for your wired computers).


# Position Your Modem Router

The modem router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your modem router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your modem router:

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the modem router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, PCs, or the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.
- With the antennas in a vertical position to provide the best side-to-side coverage or in a horizontal position to provide the best up-and-down coverage, as applicable.

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

# ADSL Microfilters

If this is the first time you have cabled a router between a DSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your Modem Router* on page 14.

An ADSL microfilter is a small in-line device that filters DSL interference out of standard phone equipment that shares the same line with your DSL service. Every telephone device that connects to a telephone line that provides DSL service needs an ADSL microfilter to filter out the DSL interference. Example devices are telephones, fax machines, answering machines, and caller ID displays. Note that not every phone line in your home necessarily carries DSL service. That depends on the DSL service setup in your home.

**Note:** Often the ADSL microfilter is in the box with the modem router. If you purchased the modem router in a country where a microfilter is not included, you have to acquire the ADSL microfilter separately.

## One-Line ADSL Microfilter

Plug the ADSL microfilter into the wall outlet and plug your phone equipment into the jack labeled Phone. The modem router plugs directly into a separate DSL line. Plugging the modem router into the phone jack blocks the Internet connection. If you do not have a separate DSL line for the modem router, the best thing to do is to use an ADSL microfilter with a built-in splitter (see *Two-Line ADSL Microfilter*)..


Plugs into DSL line

**Figure 4. One-line ADSL microfilter**

If you do not have a separate DSL line for the modem router, the second-best solution is to get a separate splitter. To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

## Two-Line ADSL Microfilter

Use an ADSL microfilter with a built-in splitter when there is a single wall outlet that provides connectivity for both the modem router and your telephone equipment. Plug the ADSL

microfilter into the wall outlet, plug your phone equipment into the jack labeled Phone, and plug the modem router into the jack labeled ADSL.


**Figure 5. Two-line ADSL microfilter with built-in splitter**

## Summary

- One-line ADSL microfilter. Use with a phone or fax machine.
- Splitter. Use with a one-line ADSL microfilter to share an outlet with a phone and the modem router.
- Two-line ADSL microfilter with built-in splitter. Use to share an outlet with a phone and the modem router.

# Cable Your Modem Router

The installation guide that came in the box has a cabling diagram on the first page. This section walks you through cabling with detailed illustrations.

**CAUTION:**

Incorrectly connecting a filter to your modem router blocks your DSL connection.

1. Put an ADSL microfilter between the phone line and the phone as shown here. The illustration shows a two-line ADSL microfilter with built-in splitter.

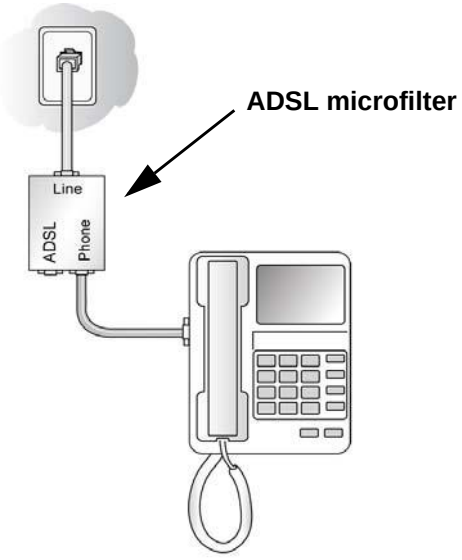



**Figure 6. ADSL microfilter between the phone line and the phone**

2. Use the included phone cable with RJ-11 jacks to connect the ADSL port (A) of the modem router to the ADSL port (B) of the two-line ADSL microfilter.

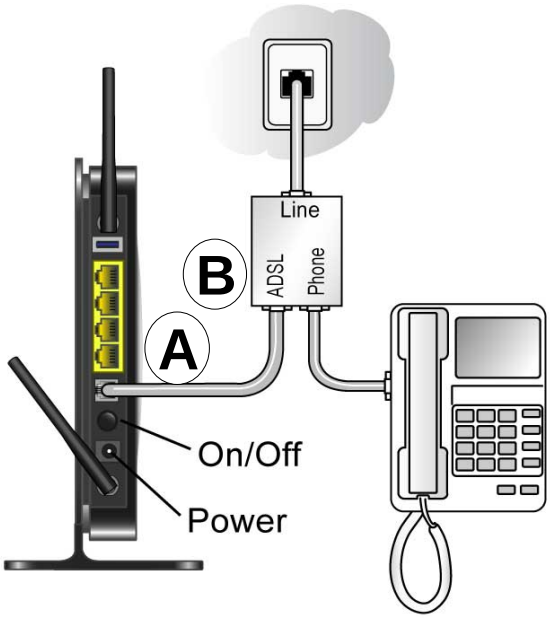



**Figure 7. Cable the modem modem router to the microfilter**

3. Connect the Ethernet cable from a modem router LAN port (C) to an Ethernet port (D) in your computer.

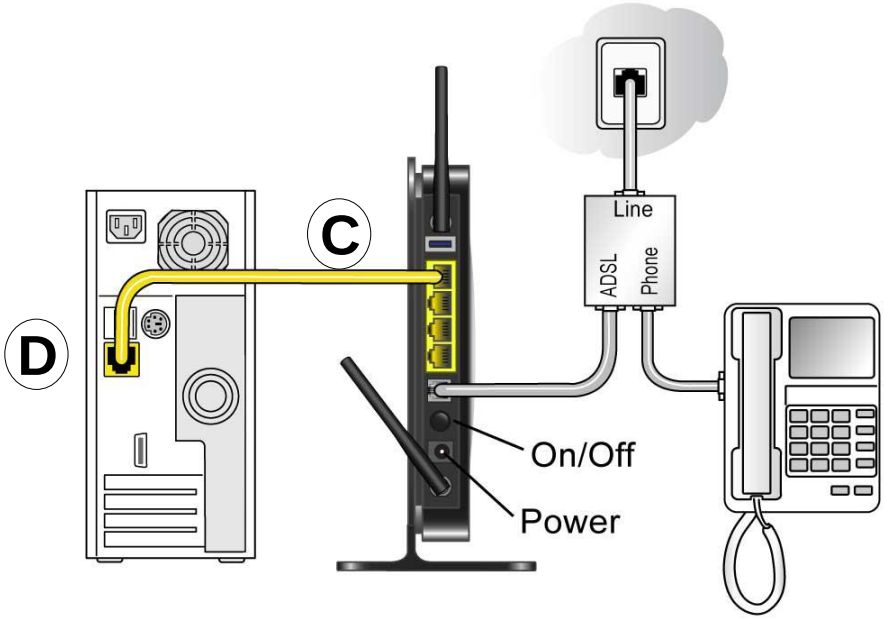



**Figure 8. Connect the Ethernet cable**

4. Plug the power adapter into the AC power adapter input (labeled Power), and plug the other end into a power outlet.

5. Connect any additional wired PCs to your modem router by inserting an Ethernet cable from a PC into one of the three remaining LAN ports.

# Verify the Cabling

Verify that your modem router is cabled correctly by checking the modem router LEDs. Turn on the modem router by pressing the **On/Off** button on the back.

- The Power LED is green when the modem routeris turned on.
- The LAN ports are green for each PC cabled to the modem router by an Ethernet cable.
- The wireless LED is green when the modem router is turned on.
- The DSL LED is green when you have a DSL connection.
- The Internet LED is red when there is no Internet connection.

Turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically.

Verify that the LAN LEDs (1 through 4) are lit for any computers cabled to the modem router by an Ethernet cable.

# 2. Modem Router Setup

This chapter explains how to set up your Internet connection using one of three methods: NETGEAR Genie®, Setup Wizard, or manual setup. If you have already set up your modem router using one of these methods, the initial setup is complete. Refer to this chapter if you want to become familiar with the modem router menus, view or adjust the initial settings, or change the modem router password and login time-out.

This chapter contains the following sections:

# Modem Router Setup Preparation

You can set up your modem router with the NETGEAR Genie as described in *NETGEAR Genie Setup* on page 19, with the Setup Wizard as described in *Setup Wizard* on page 22, or manually as described in *Manual Setup (Basic Settings)* on page 23. However, before you start the setup process, you need to have your ISP information and to make sure the laptops, PCs, and other devices in the network have the settings described here.

**Note:** For a Macintosh or Linux system, you have to use manual setup.

## Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, you have to change the settings back so that it uses Dynamic Host Configuration Protocol (DHCP).

## Replace an Existing Modem and Router

To replace an existing modem and router, disconnect them and set them aside before starting the modem router setup.

## Gather ISP Information

You need the following information to set up your modem router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your modem router Internet connection is set up, you no longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in.

- Active Internet service provided by a DSL account
- The ISP configuration information for your DSL account
  - ISP login name and password
  - ISP Domain Name Server (DNS) addresses
  - Fixed or static IP address
  - Host and domain names
  - Depending on how your ISP set up your Internet account, you could need to know one or more of these settings for a manual setup:
    - Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters
    - Multiplexing method
    - Host and domain names

# NETGEAR Genie Setup

NETGEAR Genie is on the *Resource CD* and runs on a PC with Microsoft Windows 7, Windows Vista, Windows XP, or Windows 2000 with Service Pack 2 or later. It is the easiest way to set up the modem router because it automates many steps and verifies that those steps have been successfully completed. It takes about 15 minutes to complete.

Before running NETGEAR Genie on a corporate PC, check with your company's network support staff. Corporate network settings or virtual private network (VPN) client software might conflict with your modem router settings. To avoid a conflict, use another PC.

1. Locate the DSL settings information (user name and password) provided by your ISP. Contact your ISP if you do not have it.
2. Insert the *Resource CD* into your Windows PC. The CD starts and detects the language you are using on your PC. Select a different language option, if you prefer.

   If the CD does not start, go to the CD drive (under My Computer on Windows), browse the CD, and double-click .
3. When the Welcome screen displays, click **Setup** to start the genie. Follow the instructions to complete the setup. NETGEAR Genie checks your hardware setup and guides you through connecting the modem router to the Internet and adding computers to your network.

   Your modem router connects to the Internet when any computer on your network launches a Web browser to access the Internet. The modem router's Internet LED blinks.

## View or Change Settings

You can view and change the settings in the following ways:

- Log in to your modem router. To do this you can click the shortcut that was placed on your desktop during the NETGEAR Genie setup, or use an Internet browser. See *Log In to the Modem Router* on page 20.
- Open the Router_Setup.html file that was placed on your desktop during the NETGEAR Genie setup. This file has setup and system information, the NETGEAR Technical Support phone number, links to the NETGEAR website, and a modem router login link.

## Settings Description

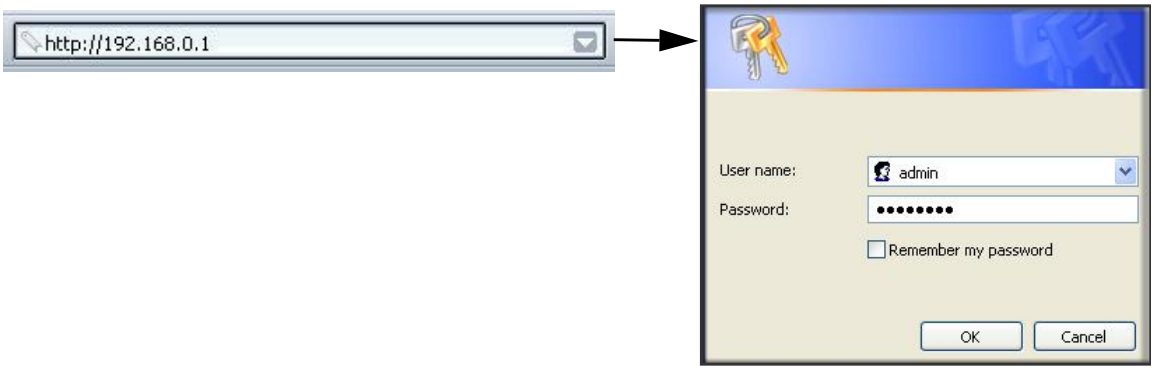
When the NETGEAR Genie is done, your modem router has the following settings. Some of these can be viewed in Router_Setup.html.

- Language and country as described in *Setup Wizard* on page 22.
- Internet connection settings as described in *Table 2, Basic Settings Screen Description* on page 24.
- Network settings. The NETGEAR Genie steps you through connecting from your computer to the modem router.

# Log In to the Modem Router

Log in to the modem router to view or change settings or to set up the modem router.

1. Type **http://192.168.0.1** in the address field of your browser and press **Enter** to display the login window. You can also enter either of these addresses to access the modem router: **http://www.routerlogin.net** or **http://www.routerlogin.com**.




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

> **Note:** The modem router user name and password are probably different from the user name and password for logging in to your Internet connection. See *Types of Logins* on page 28 for more information.

The modem router screen displays as described in *Modem Router Interface* on page 21.

If you do not see the login prompt:

1. Check the LEDs on the modem router front panel to make sure that the modem router is plugged into an electrical outlet, its power is on, and the Ethernet cable between your computer and the modem router is connected to a LAN port.
2. If you connected the Ethernet cable and quickly launched your browser and typed in the modem router URL, your computer might need a minute or two to recognize the LAN connection. Relaunch your browser and try again.
3. If you are having trouble accessing the modem router wirelessly, NETGEAR recommends that during setup you use an Ethernet cable to connect your computer so that you can log in to the modem router.
4. If you cannot connect to the modem router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain both IP and DNS server addresses automatically. See your computer documentation.

# Upgrade Modem Router Firmware

When you log in, if you are connected to the Internet, the Firmware Upgrade Assistant screen displays so you can upgrade to the latest firmware. See *Chapter 5, Network Maintenance*, for more information about upgrading firmware.

1. Click **Yes** to check for new firmware (recommended). The modem router checks the NETGEAR database for new firmware.
2. If no new firmware is available, click **No** to exit. You can check for new firmware later.
3. If new firmware is available, click **Yes** to upgrade the modem router with the latest firmware. After the upgrade, the modem router restarts.

**CAUTION:**

Do not try to go online, turn off the modem router, shut down the computer, or do anything else to the modem router until the modem router finishes restarting and the Ready light has stopped blinking for several seconds.

You cannot upgrade firmware until you have established your Internet connection as described in *Setup Wizard* on page 22.

# Modem Router Interface

The modem router interface lets you view or change the modem router settings. The left column has menus, and the right column provides online help. The middle column is the screen for the current menu option.

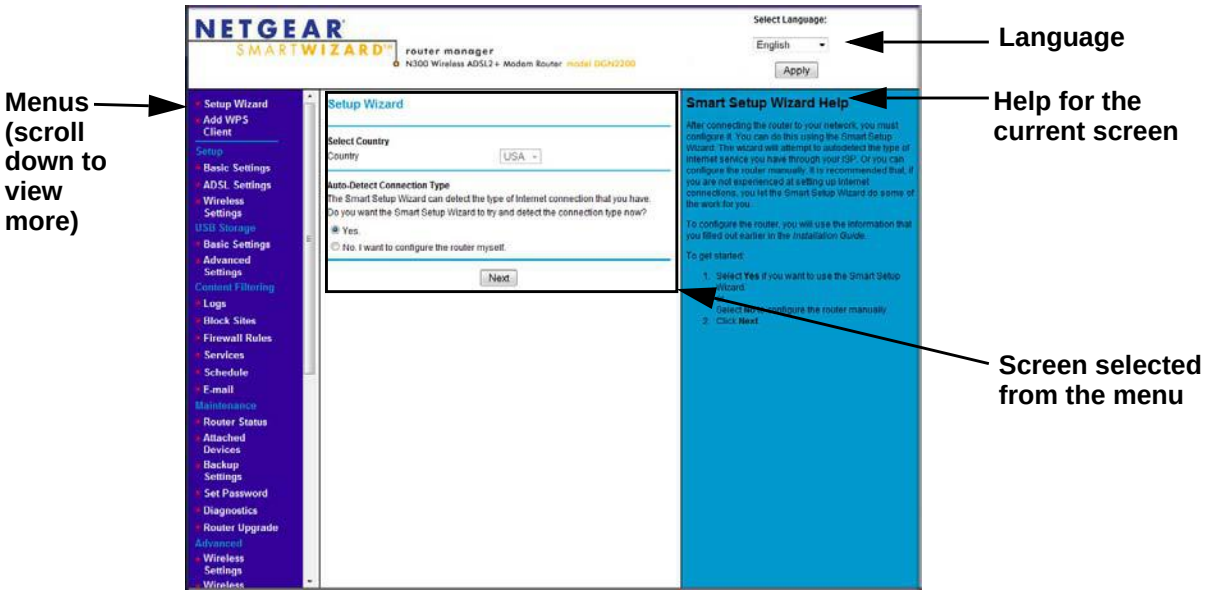



**Figure 9. Modem Router interface**

- **Setup Wizard**. Specify the language and location, and automatically detect the Internet connection. See *Setup Wizard* on page 22.
- **Add WPS Client**. Add WPS-compatible wireless devices and other equipment to your wireless network. See *Add Clients (Computers or Devices) to Your Network* on page 31.
- **Setup menu**. Set, upgrade, and check the ISP and wireless network settings of your modem router. See *Manual Setup (Basic Settings)* on page 23 and *ADSL Settings* on page 26. See also *Chapter 3, Wireless Settings*, for information about preset and basic security settings.
- **Content Filtering menu**. View and configure the modem router firewall settings to prevent objectionable content from reaching your PCs. See *Chapter 4, Content Filtering Settings*.
- **Maintenance menu**. Administer and maintain your modem router and network. See *Chapter 5, Network Maintenance*.
- **Advanced menu**. Set the modem router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 7, Advanced Settings*. Using this menu requires a solid understanding of networking concepts.
- **Advanced VPN menu**. Set up virtual private networking (VPN) features of the modem router. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer. See *Chapter 7, Virtual Private Networking*.
- **Web Support**. Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

# Setup Wizard

If you do not use the NETGEAR Genie, you have to log in to the modem router to set the country, language, and Internet connection. If you performed the NETGEAR Genie setup, the country, language, Internet, and wireless network settings are already configured.

1. From the top of the modem router menu, select **Setup Wizard** to display the following screen:


2. Select your country.

It is important to specify the location where the modem router operates so that the Internet connection works correctly.

3. Select either **Yes** or **No, I want to configure the Router myself**. If you select No, proceed to *Manual Setup (Basic Settings)* on page 23.
4. If you selected Yes, click **Next**.

   With automatic Internet detection, the Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

**Note:** The Setup Wizard cannot detect a Point-to-Point Tunneling Protocol (PPTP) connection. If your ISP uses PPTP, you have to set your Internet connection through the screen described in *Manual Setup (Basic Settings)* on page 23.

# Manual Setup (Basic Settings)

The Basic Settings screen displays when you select No. I want to configure the Router myself in the Setup Wizard and is also available from the modem router menu. It is where you view or change ISP information. The fields that display vary depending on whether or not your Internet connection requires a login.

**Note:** Check that the country is set as described *Setup Wizard* on page 22 before proceeding with the manual setup.

1. Select **Set Up > Basic Settings,** and select **Yes** or **No** depending on whether or not your ISP requires a login. *Figure 10, Basic Settings screen without (left) and with (right) login.* shows both forms of the Basic Settings screen.
   - **Yes**. Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. Enter the account and domain names, as needed.
2. Enter the settings for the IP address and DNS server. The default DSL settings usually work fine. If you have problems with your connection, check the DSL settings, and see *ADSL Settings* on page 26 for more information.
3. If no login is required, you can specify the MAC Address setting.
4. Click **Apply** to save your settings.

5. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within 1 minute, and see *Troubleshooting* on page 128.

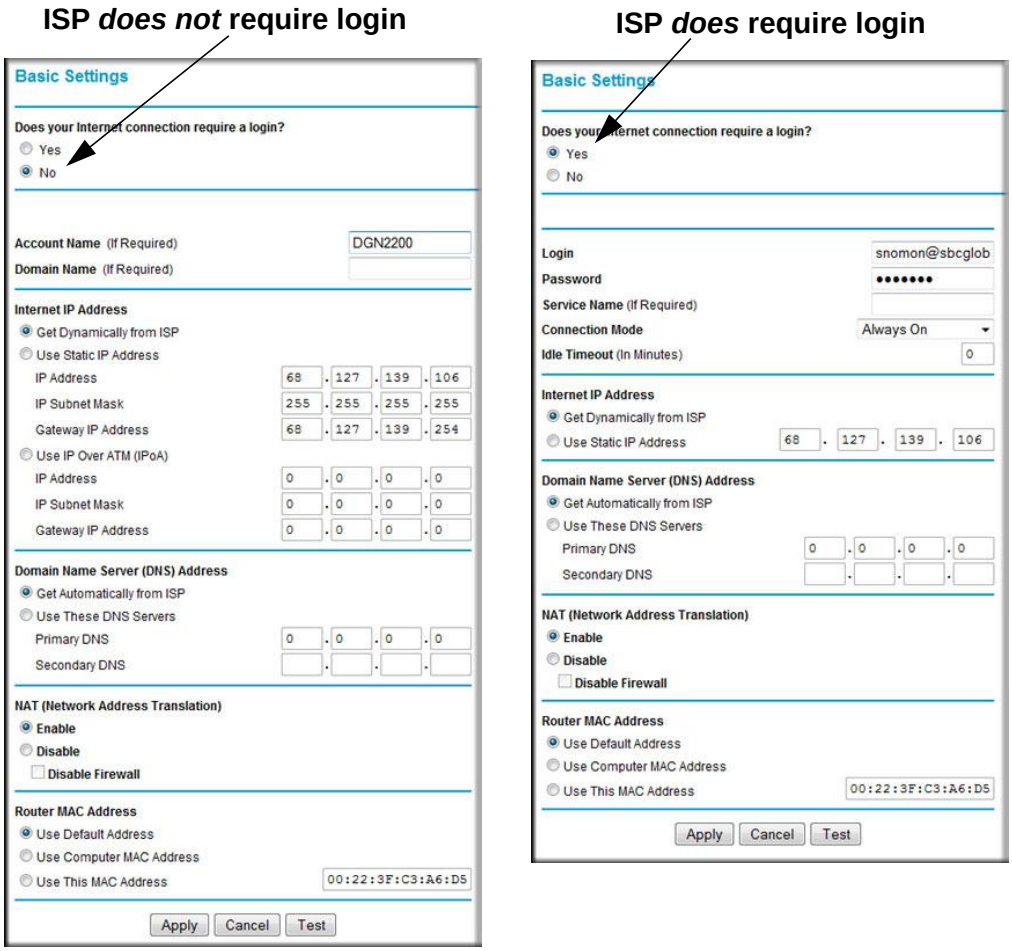



**Figure 10. Basic Settings screen without (left) and with (right) login.**

The following table explains all the possible fields in the Basic Settings screen. Note that which fields appear in this screen depends on whether or not a login is required.

**Table 2. Basic Settings Screen Description**

| Settings | | Description |
|---|---|---|
| Does Your ISP Require a Login? | | • Yes<br>• No |
| These fields display only if no login is required. | Account Name (If required) | Enter the account name provided by your ISP. This might be called the host name. |
| | Domain Name (If required) | Enter the domain name provided by your ISP. |

**Table 2. Basic Settings Screen Description**

| Settings | | Description |
|---|---|---|
| These fields display only if your ISP requires a login. | Encapsulation | Encapsulation is a method for enclosing multiple protocols. PPP stands for Point-to-Point Protocol. The choices are:<br>• PPPoE (PPP over Ethernet)<br>• PPPoA (PPP over ATM) |
| | Login | The login name provided by your ISP. This is often an email address. |
| | Password | The password that you use to log in to your ISP. |
| | Idle Timeout (In minutes) | The number of minutes the modem router keeps the Internet connection active after there is no Internet activity from the LAN. You can enter a new value in minutes. Zero (0) means never log out. |
| Internet IP Address | | • **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.<br>• **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's gateway to which your modem router will connect. |
| | This field displays only if no login is required. | **Use IP Over ATM (IPoA)**. Your ISP uses classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned. |
| Domain Name Server (DNS) Address | | The DNS server looks up website addresses based on their names.<br>• **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers automatically.<br>• **Use These DNS Servers**. If you know that your ISP does not send DNS addresses to the modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. |
| NAT (Network Address Translation) | | NAT assigns private IP addresses (10.1.1.x) to LAN-connected devices.<br>• **Enable**. Usually NAT is enabled.<br>• **Disable**. Disable NAT, but leave the firewall active. Disable NAT only if you are technically skilled and are sure you do not need it.[1]<br>• **Disable firewall**. This disables the firewall and NAT. This removes the usual protection for your network. |
| Router MAC Address | | The Ethernet MAC address used by the modem router Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from that MAC address.<br>• **Use Default Address**. Use the default MAC address.<br>• **Use Computer MAC Address**. Copy (clone) the MAC address of the computer that you are now using and use that for the ISP. You have to use the computer that is allowed by the ISP.<br>• **Use This MAC Address**. Enter the MAC address you want to use. |

*1. Disabling NAT reboots the modem router and restores its factory default settings. Disable NAT only if you plan to manually administer the IP address space on the LAN side of the modem router.*

# ADSL Settings

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

**Note:** You have to use the Setup Wizard to select the correct country for the default DSL settings to work.

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

1. Select **Setup > ADSL Settings** to display the following screen:


2. In the Multiplexing Method drop-down list, select **LLC-based** or **VC-based**.
3. For the VPI, type a number between 0 and 255. The default is 8 for the U.S. version, 0 for the world wide version, and 1 for the German version.
4. For the VCI, type a number between 32 and 65535. The default is 35 for the U.S. version, 38 for the worldwide version, and 32 for the German version.
5. Click **Apply**.

# Unsuccessful Internet Connection

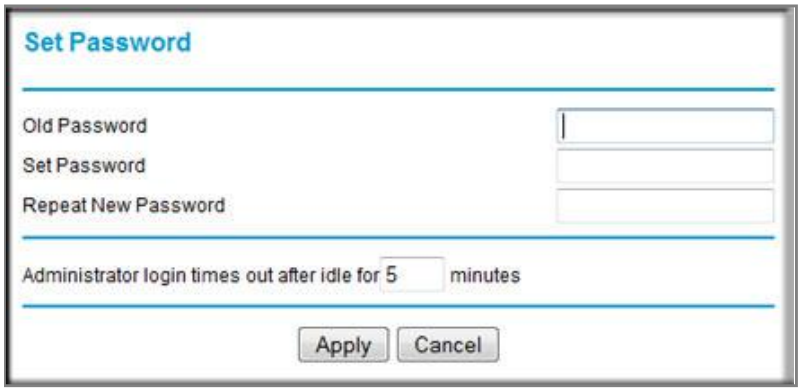
1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 9, Troubleshooting*. If problems persist, register your NETGEAR product and contact NETGEAR Technical Support.
4. If you cannot connect to the modem router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your PC Control Panel. They should be set to obtain *both* IP and DNS server addresses automatically. See your computer documentation.

# Change Password and Login Time-Out

For security reasons, the modem router has its own user name and password that default to admin and password. You can and should change these to a secure user name and password that are easy to remember. The ideal password contains no dictionary words from any language and is a mixture of upper case and lower case letters, numbers, and symbols. It can be up to 30 characters.

**Note:** The modem router user name and password are not the same as the user name and password for logging in to your Internet connection. See *Types of Logins* on page 28 for more information about login types.

1. Select **Maintenance > Set Password** to display the following screen:.




2. Enter the old password.
3. Enter the new password twice.
4. Change the login time-out to a value between 1 and 99 minutes if the default value of 5 minutes does not meet your needs.

   The administrator's login to the modem router configuration times out after a period of inactivity to prevent someone else from accessing the modem router interface when you step away.

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

   After changing the password, you are required to log in again to continue the configuration. If you have backed up the modem router settings previously, you should do a new backup so that the saved settings file includes the new password. See *Back Up* on page 56 for information about backing up your network configuration.

# Log Out Manually

The modem router interface provides a Logout command at the bottom of the modem router menus. Log out when you expect to be away from your computer for a relatively long period of time.

# Types of Logins

There are three separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

- **Modem router login** logs you in to the modem router interface. See *Log In to the Modem Router* on page 20 for details about this login.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wi-Fi network name and passphrase** logs you in to your wireless network. This login is preconfigured and can be found on the label on the bottom of your unit. See *Chapter 3, Wireless Settings*, for more information.

# Wireless Settings

## Protecting your network

3

This chapter describes how to use the Wireless Settings screens to view and change (if needed) your wireless network settings. Security features to prevent objectionable content from reaching your PCs are covered in *Chapter 4, Content Filtering Settings*.

This chapter contains the following sections:



## Wireless Adapter Compatibility

A wireless adapter is the wireless radio in your PC or laptop that lets the PC or laptop connect to a wireless network. Most PCs and laptops come with an adapter already installed, but if it is outdated or slow, you can purchase a USB adapter to plug into a USB port.

Make sure the wireless adapter in each computer in your wireless network supports the same security settings as the modem router. See *Preset Security* on page 30 for information about the modem router's preconfigured security settings.

**Note:** If you connect devices to your modem router using WPS as described in *Wi-Fi Protected Setup (WPS) Method* on page 32, those devices assume the security settings of the modem router.

# Preset Security

The modem router comes with preset security. This means that the Wi-Fi network name (SSID), passphrase, and security option (encryption protocol) are preset in the factory. You can find the preset SSID and passphrase on the bottom of the unit.

- **Wi-Fi network name (SSID)** identifies your network so devices can find it.
- **Passphrase** controls access to your network. Devices that know the SSID and the passphrase can find your wireless network and connect.

**Note:** The preset SSID and passphrase are uniquely generated for every device to protect and maximize your wireless security.

- **Security option** is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. The preset security option is WPA-PSK/WPA2-PSK mixed mode, described in *Wireless Security Options* on page 31.

The Wireless Settings screen lets you view and change the preset security settings. ***However, NETGEAR recommends that you not change your preset security settings***. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

# Security Basics

Unlike wired network data, wireless data transmissions extend beyond your walls and can be received by any device with a compatible wireless adapter (radio). For this reason, it is very important to maintain the preset security and understand the other security features available to you. Besides the preset security settings described in the previous section, your modem router has the security features described here and in *Chapter 4, Content Filtering Settings*.

- Turn off wireless connectivity
- Disable SSID broadcast
- Restrict access by MAC address
- Wireless security options

## Turn Off Wireless Connectivity

You can turn off the wireless connectivity of the modem router by pressing the Wireless **On/Off** button on its front panel  . For example, if you use your laptop to wirelessly connect to your modem router and you take a business trip, you can turn off the wireless portion of the modem router while you are traveling. Other members of your household who use computers connected to the modem router through Ethernet cables can still use the modem router.

## Disable SSID Broadcast

By default, the modem router broadcasts its Wi-Fi network name (SSID) so devices can find it. If you change this setting to not allow the broadcast, wireless devices will not find your modem router unless they are configured with the same SSID. See *Wireless Access Point Settings* on page 35 for the procedure.

**Note:** Turning off SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. If you allow the broadcast, be sure to keep wireless security enabled.

## Restrict Access by MAC Address

You can enhance your network security by allowing access to only specific PCs based on their Media Access Control (MAC) addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the modem router. The Wireless Station MAC address filtering adds additional security protection to the wireless security option that you have in force. The Access list determines which wireless hardware devices are allowed to connect to the modem router by MAC address. See *Advanced Wireless Settings* on page 79 for the procedure.

## Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are several types of encryption: Wi-Fi Protected Access II (WPA2), WPA, and Wired Equivalent Privacy (WEP). WPA2 is the latest and most secure, and is recommended if your equipment supports it. WPA has several options including pre-shared key (PSK) encryption and 802.1x encryption for enterprises. Note that it is also possible to disable wireless security. NETGEAR does *not* recommend this. You can view or change the wireless security options in the Wireless Settings screen. See *Wireless Settings Screen* on page 33.

# Add Clients (Computers or Devices) to Your Network

Choose either the manual or the WPS method to add wireless computers or devices to your wireless network.

## Manual Method

1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your modem router. This software scans for all wireless networks in your area.
2. Look for your network and select it. If you did not change the name of your network during the setup process, look for the default Wi-Fi network name (SSID) and select it. The default Wi-Fi network name (SSID) is located on the product label on the bottom of the modem router.
3. Enter the modem router passphrase and click **Connect**. The default modem router passphrase is located on the product label on the bottom of the modem router.
4. Repeat steps 1–3 to add other wireless devices.

## Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) is a standard that lets you easily join a secure wireless network with WPA or WPA2 wireless security. The modem router automatically sets security for each computer or device that uses WPS to join the wireless network. To use WPS, make sure that your wireless devices are Wi-Fi certified and support WPS. NETGEAR products that use WPS call it Push 'N' Connect.[1]

> **Note:** If the wireless network name (SSID) changes each time you add a WPS client, the Keep Existing Wireless Settings check box on the Advanced Wireless Settings screen has been cleared. See *WPS Settings* on page 80 for more information about this setting.

You can use a WPS button or the modem router interface method to add wireless computers and devices to your wireless network.

### *WPS Button Method*

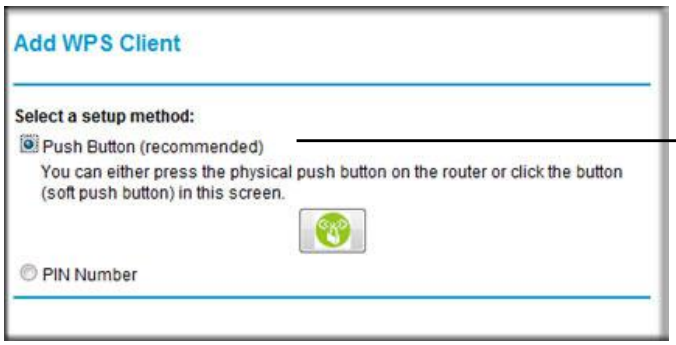
1. Press the  **WPS** button on the modem router front panel.
2. Within 2 minutes, press the **WPS** button on your wireless computer or device, or follow the WPS instructions that came with the computer. The device is now connected to your modem router.
3. Repeat steps 1–2 to add other WPS wireless computers or devices.

### *Modem Router Interface Method*

1. Select **Add WPS Client** at the top of the modem router menus.

*1. For a list of other Wi-Fi-certified products available from NETGEAR, go to http://www.wi-fi.org.*

2. Click **Next**. The following screen lets you select the method for adding the WPS client.




3. Select either **Push Button** or **PIN Number**. With either method, the modem router tries to communicate with the computer or wireless device, set the wireless security for wireless device, and allow it to join the wireless network.

   The PIN method displays this screen so you can enter the client security PIN number:


   While the modem router attempts to connect, the WPS LED on the front of the modem router blinks green. When the modem router establishes a WPS connection, the LED is solid green and the modem router WPS screen displays a confirmation message.

4. Repeat to add another WPS client to your network.

# Wireless Settings Screen

The Wireless Settings screen lets you view or change the wireless network settings. Note that your preset modem router has a unique network name and password, located on the product label. NETGEAR recommends that you use these settings. If you decide to change them, note the new settings and save them in a secure location.

**Note:** If you use a wireless computer to change the wireless network name (SSID) or security options, you are disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the modem router.

## Consider Every Device on Your Network

Before you begin, check the following:

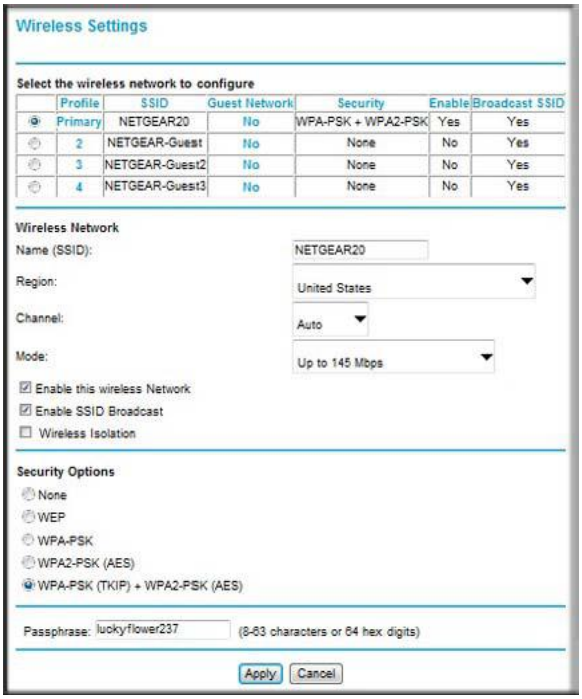
- Every wireless computer has to be able to obtain an IP address by DHCP from the modem router as described in *Use Standard TCP/IP Properties for DHCP* on page 18.
- Each computer or wireless adapter in your network must have the same SSID and wireless mode (bandwidth/data rate) as the modem router. Check that the wireless adapter on each computer can support the mode and security option you want to use.
- The security option on each wireless device in the network must match the modem router. For example, if you select a security option that requires a passphrase, be sure to use same passphrase for each wireless computer in the network.

## View or Change Wireless Settings

Your preset modem router comes set up with a unique wireless network name (SSID) and network password. This information is printed on the label for your modem router. You view or change these settings in the Wireless Settings screen. You can also use this screen to set up guest wireless networks.

### To view or change wireless settings:

1. Select **Setup > Wireless Settings** to display the following screen.




2. Select the wireless network that you want to configure.
3. Make any changes that are needed, and click **Apply** when done to save your settings.

**Note:** The screen sections, settings, and procedures are explained in the following sections.

4. Set up and test your computers for wireless connectivity:
   a. Use your wireless computer or device to join your network. When prompted, enter the network password.
   b. From the wirelessly connected computer, make sure that you can access the Internet.

# Wireless Settings Screen Fields

## *Wireless Network*

The primary network is the one that you usually use. You can set up guest networks too. You can customize access so that people who use their computers to access your guest network can use the Internet, but they do not have access to the rest of your home network.

- **Name (SSID)**. The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID for your primary network is randomly generated, and there is typically no need to change it. If you want to set up guest networks, NETGEAR does recommend that you customize the default guest network names (SSIDs).
- **Region**. The location where the modem router is used. It might not be legal to operate the modem router in a region other than the regions listed.
- **Channel**. The wireless channel used by the gateway: 1 through 13. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.
- **Mode**. Up to 150 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. Up to 65 Mbps supports up to 65 Mbps.

## *Wireless Access Point Settings*

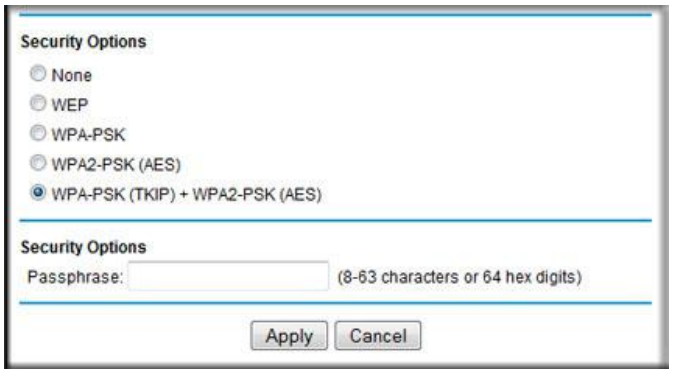
- **Enable this wireless network**. When this check box is selected, the modem router accepts wireless clients for the network. By default, this check box is selected for your primary network. If you clear this check box, the modem router accepts wired clients only.
- **Allow Broadcast of Name (SSID)**. This setting allows the modem router to broadcast its SSID so that a wireless station can display this wireless name (SSID) in its scanned network list. This check box is selected by default. To turn off the SSID broadcast, clear the **Allow Broadcast of Name (SSID)** check box and click **Apply**.
- **Wireless Isolation**. When this check box is selected, wireless stations cannot communicate with each other or with stations on the wired network. By default, this check box is not selected.

### *Security Options Settings*

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. The primary network for your preset modem router is already set up with WPA2 and WPA security. NETGEAR recommends that you set up wireless security for each guest network that you plan to use. For information about changing these settings, see the following section, *Change WPA Security Option and Passphrase*, and *Set WEP Encryption and Passphrase* on page 36.

## Change WPA Security Option and Passphrase

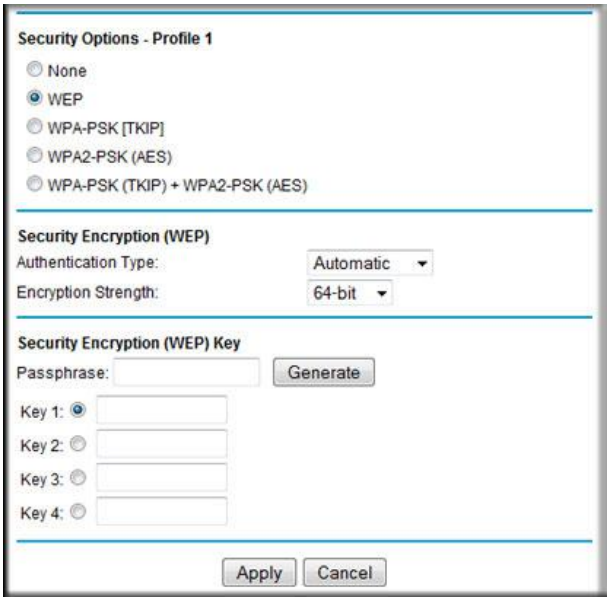
1. In the Security Options section, select the WPA option that you want.




2. Enter the passphrase that you want to use. It is a text string from 8 to 63 characters.
3. Click **Apply**.

## Set WEP Encryption and Passphrase

1. In the Security Options section of the Wireless Settings screen, select **WEP**:



2. Select the authentication type. The default is Automatic. Other choices are Open System (any client can authenticate itself to the network) and Shared Key (a passphrase and a four-way challenge are needed for authentication).
3. Select the encryption strength setting, either 64 bit or 128 bit.
4. Enter the four data encryption keys either manually or automatically. These values must be identical on all computers and access points in your network.
   - **Automatic**. Enter a word or group of printable characters in the Passphrase field and click **Generate**. The four key fields are automatically populated with key values.
   - **Manual**. The number of hexadecimal digits that you enter depends on the encryption strength setting:
     - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
     - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
5. Select the radio button for the key you want to make active.

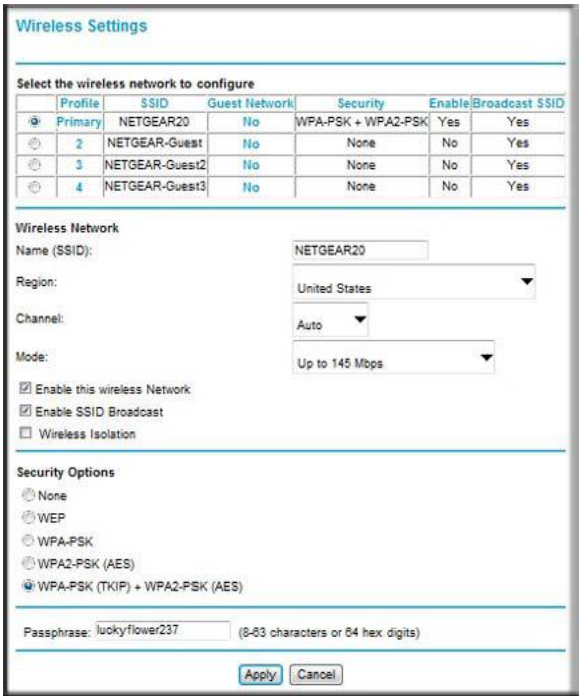
   Make sure that you understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one in Windows XP allow one key entry, which has to match the default key you set in the modem router.
6. Click **Apply**.

# Wireless Guest Networks

A wireless guest network allows you to provide guests access to your wireless network without prior authorization of each individual guest. You can configure wireless guest networks and specify the security options for each wireless guest network.

### To set up a wireless guest network:

1. Select **Setup > Wireless Settings**.




2. Select the radio button for the network profile that you want to set up.
3. You can specify whether the SSID broadcast is enabled, and whether you want to allow the guest to access your local network. You can also change the SSID.
   - NETGEAR strongly recommends that you change the SSID to a different name. Note that the SSID is case-sensitive. For example, GuestNetwork is not the same as Guestnetwork.
   - For guest networks, wireless security is disabled by default. NETGEAR strongly recommends that you implement wireless security for the guest network.
4. Select a security option for the guest network and specify the password.
5. When you have finished making changes, click **Apply**.

# Content Filtering Settings

# 4

## Keeping unwanted content out of your network

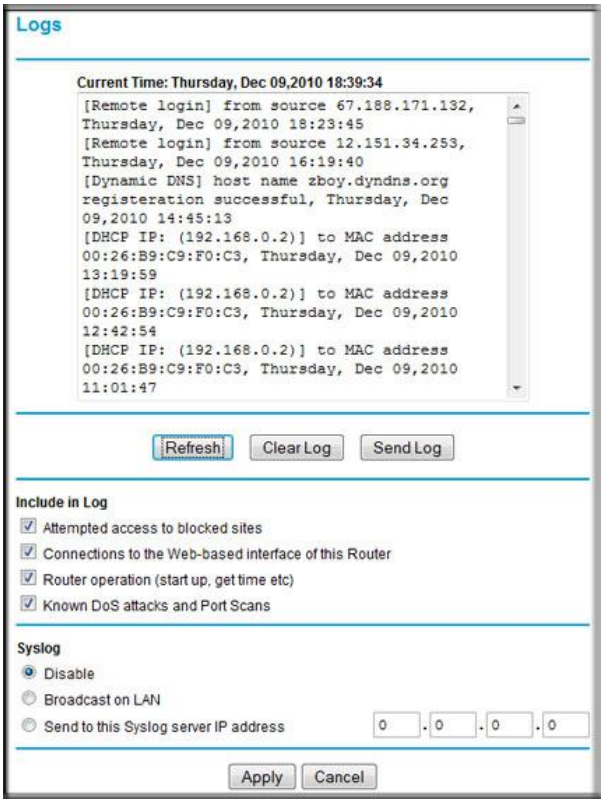
This chapter explains how to use the basic firewall features of the modem router to prevent objectionable content from reaching the PCs and other devices connected to your network.

This chapter contains the following sections:

# Logs

The modem router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites screen, the Logs screen show you when someone on your network tries to access a blocked site. If you enable email notification, you will receive these logs in an email message.

To view the log, select **Content Filtering > Logs**. A screen similar to the following displays:




The Include in Log check boxes allow you to select which events are logged. You can write the logs to a computer running a syslog program. To activate this feature, select **Broadcast on LAN**, or enter the IP address of the server where the syslog file will be written. The security log entries include the following information:

- **Date and time**.The date and time the log entry was recorded.
- **Description or action**. The type of event and what action was taken, if any.
- **Source IP**. The IP address of the initiating device for this log entry.
- **Source port and interface**. The service port number of the initiating device, and whether it originated from the LAN or WAN.
- **Destination**. The name or IP address of the destination device or website.
- **Destination port and interface**. The service port number of the destination device, and whether it is on the LAN or WAN.

# Examples of Log Messages

Following are examples of log messages. In all cases, the log entry shows the time stamp as day, year-month-date  hour:minute:second.

## *Activation and Administration*

```
Tue, 2006-05-21 18:48:39 - NETGEAR activated
```

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

```
Tue, 2006-05-21 18:55:00 - Administrator login successful-IP:192.168.0.2
Thu, 2006-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

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

```
Tue, 2006-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

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

```
Wed, 2006-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was emailed.]

## *Dropped Packets*

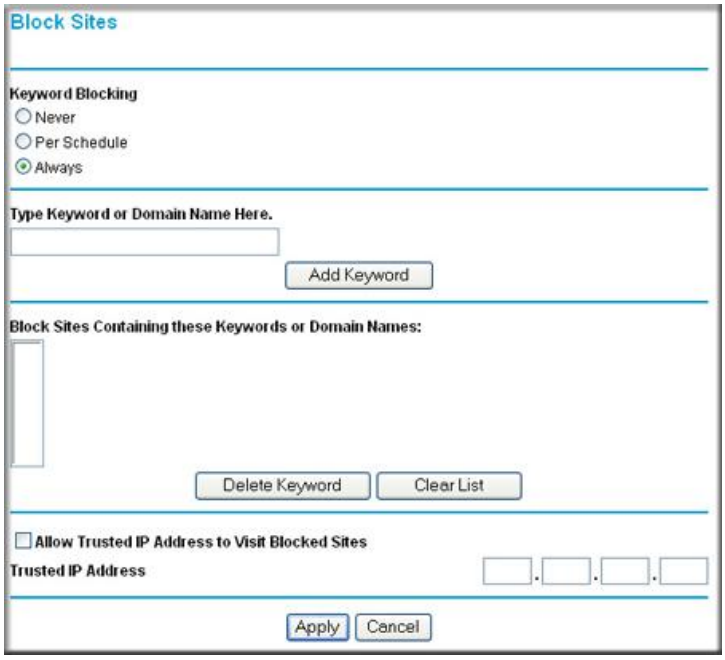
```
Wed, 2006-05-22 07:15:15 - TCP packet dropped -
Source:64.12.47.28,4787,WAN - Destination:134.177.0.11,21,LAN - [Inbound
Default rule match]
Sun, 2006-05-22 12:50:33 - UDP packet dropped -
Source:64.12.47.28,10714,WAN - Destination:134.177.0.11,6970,LAN -
[Inbound Default rule match]
Sun, 2006-05-22 21:02:53 - ICMP packet dropped -
Source:64.12.47.28,0,WAN - Destination:134.177.0.11,0,LAN - [Inbound Default rule
match]
```

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

# Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a scheduled.

1. Select **Security > Block Sites**.




2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the Keyword field, enter a keyword or domain, click **Add Keyword,** and click **Apply**.

   The Keyword list. supports up to 32 entries. Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (**.**) to block all Internet browsing access.

## Delete Keyword or Domain

1. Select the keyword or domain that you want to delete from the list.
2. Click **Delete Keyword** and click **Apply** to save your changes.

## Specify Trusted Computer

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply** to save your changes.

# Firewall Rules to Control Network Access

Your modem router has a firewall that blocks unauthorized access to your wireless network and permits authorized inbound and outbound communications. Authorized communications are established according to inbound and outbound rules. The firewall has the following two default rules. You can create custom rules to further restrict the outbound communications or more widely open the inbound communications:

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

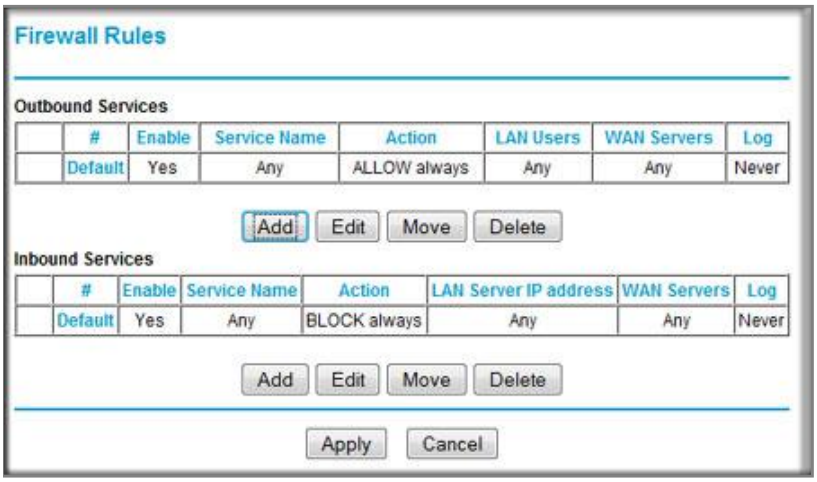
## Configure Firewall Rules

The Firewall Rules screen lets you configure custom rules to make exceptions to the default rules. Exceptions can be based on the service or application, source or destination IP addresses, and time of day. You can log traffic that matches or does not match the rule and change the order of rule precedence. See *Set Up Services* on page 48 for information about services.

All traffic attempting to pass through the firewall is subjected to the rules in the order shown in the Rules table from the top (highest precedence) to the default rules at the bottom. In some cases, the order of precedence is important to determine which communications are allowed into or out of the network.

### To set up firewall rules:

1. Select **Security > Firewall Rules** to display the following screen:




2. To add an inbound or outbound rule:
   - For an outbound rule, click **Add** under Outbound Services.
   - For an inbound rule, click **Add** under Inbound Services.
3. To edit or delete a rule, select its button on the left side and click **Edit** or **Delete**.
4. To change the order of precedence:
   a. Select its button on the left side of the table and click **Move**.
   b. At the prompt, enter the number of the new position and click **OK**.
5. To open or close instant messaging, select one of the following radio buttons:
   - **Close IM Ports**. Disables instant messaging traffic.
   - **Open IM Ports**. Enables instant messaging traffic. IM ports are open by default.
6. Click **Apply** to save your settings.

## Inbound Rules (Port Forwarding)

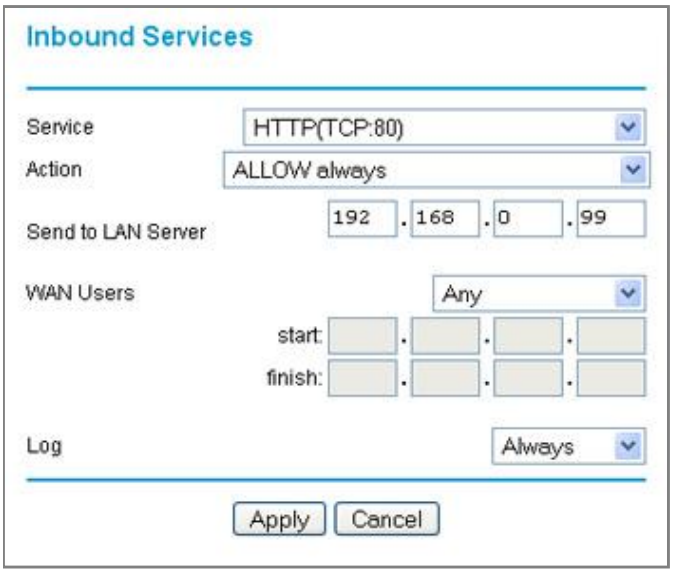
Because the modem router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet.

The rule tells the modem router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding. Allowing inbound services opens holes in your firewall. Enable only those ports that are necessary for your network. The following are two examples of inbound rules.

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

## *Inbound Rule Example: A Local Public Web Server*

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day, as shown here and described following the figure:




The settings are:

- **Service**. From this list, select the application or service you want to allow or block. The list already displays many common services, but you are not limited to these choices. Use the Services screen to add any additional services or applications that do not already appear. See *Set Up Services* on page 48.
- **Action**. Choose how you want to handle this type of traffic. You can block or allow always, or you can block or allow according to the schedule you have defined in the Schedule screen, described in *Schedule Services* on page 50.
- **Send to LAN Server**. Enter the IP address of the computer or server on your LAN that receives the inbound traffic covered by this rule.
- **WAN Users**. These settings determine which packets are covered by the rule, based on their source (WAN) IP address:
  - **Any**. All IP addresses are covered by this rule.
  - **Address range**. If this option is selected, you must fill in the Start and Finish fields.
  - **Single address**. Enter the required address in the Start field.

- **Log**. You can select whether to log the traffic:
  - **Never**. No log entries are made for this service.
  - **Always**. Any traffic for this service type is logged.
  - **Match**. Traffic of this type that matches the settings and action are logged.
  - **Not match**. Traffic of this type that does not match the settings and action are logged.

## *Inbound Rule Example: Allowing Video Conferencing*

Create an inbound rule to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office. In the following figure, CU-SeeMe connections are allowed from a specified range of external IP addresses only. In this case, incoming CU-SeeMe requests that do not match the allowed settings are logged.

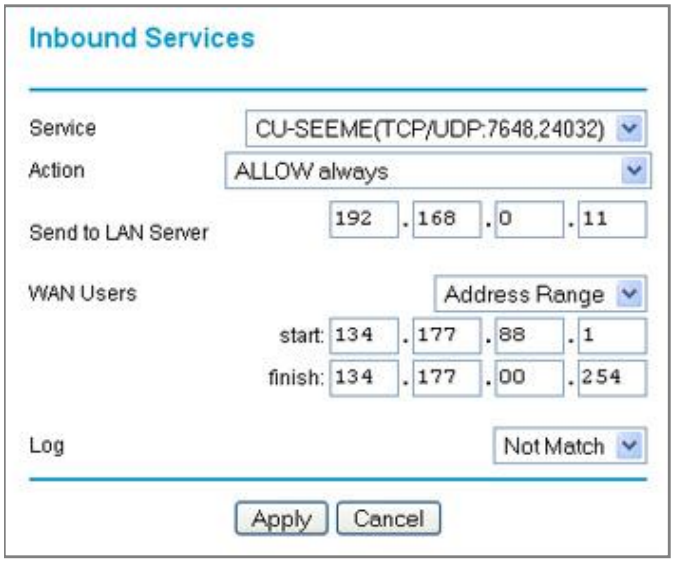



**Figure 11. Inbound video conferencing**

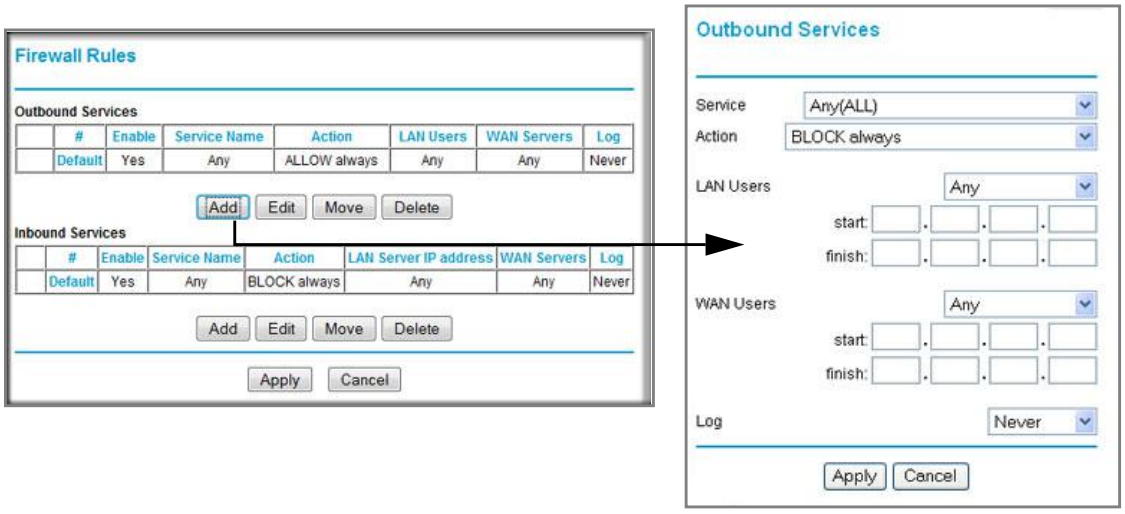
## *Considerations for Inbound Rules*

- If your external IP address is assigned dynamically by your ISP, the IP address might change periodically as the DHCP lease expires. Consider using the Dynamic DNS screen described in *Dynamic DNS* on page 75 so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it might change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP Setup screen to keep the computer's IP address constant.
- Local computers must access the local server using the computer's local LAN address (192.168.0.11 in the example shown in *Figure 11, Inbound video conferencing*). Attempts by local computers to access the server using the external WAN IP address fail.

# Outbound Rules (Service Blocking)

You can block computers on your local network from using certain Internet services. This is called service blocking or port filtering. You can add an outbound rule to block Internet access from a local computer based on the computer, Internet site, time of day, and type of service.

1. Select **Security > Firewall Rules** to display the following screen:




2. Under Outbound Services, click **Add.**
3. Fill in the fields as follows and click **Apply** to save your settings:
   - **Service**. Select the application or service to be allowed or blocked. The list has many services, but you are not limited to these choices. You can use the **Add Custom Service** button (see *Set Up Services* on page 48) to add services or applications.
   - **Action**. Choose how to handle this type of traffic. You can block or allow always, or according to the schedule you define. (See *Schedule Services* on page 50.)
   - **LAN Users**. These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the option that you want:
     - **Any**. All IP addresses are covered by this rule.
     - **Address range**. If this option is selected, fill in the Start and Finish fields.
     - **Single address**. Enter the required address in the Start field.
   - **WAN Users**. These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the option that you want:
     - **Any**. All IP addresses are covered by this rule.
     - **Address range**. If this option is selected, fill in the Start and Finish fields.
     - **Single address**. Enter the required address in the Start field.
   - **Log**. You can select to log the traffic:
     - **Never**. No log entries are made for this service.
     - **Always**. Any traffic for this service type is logged.
     - **Match**. Traffic of this type that matches the settings and action is logged.
     - **Not match**. Traffic that does not match the settings and action is logged.

# Set Up Services

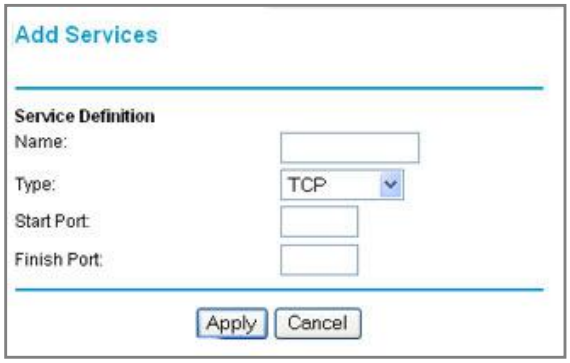
Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server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

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF at *http://www.ietf.org/*) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. Although the modem router already holds a list of many service port numbers, you are not limited to these choices.

### To create your own service definitions:

1. Select **Security > Services** to display the following screen:


2. To create a new service, click the **Add** button. If you want to change a service, select it and click **Edit**.
3. Use the following screen to define or edit a service.

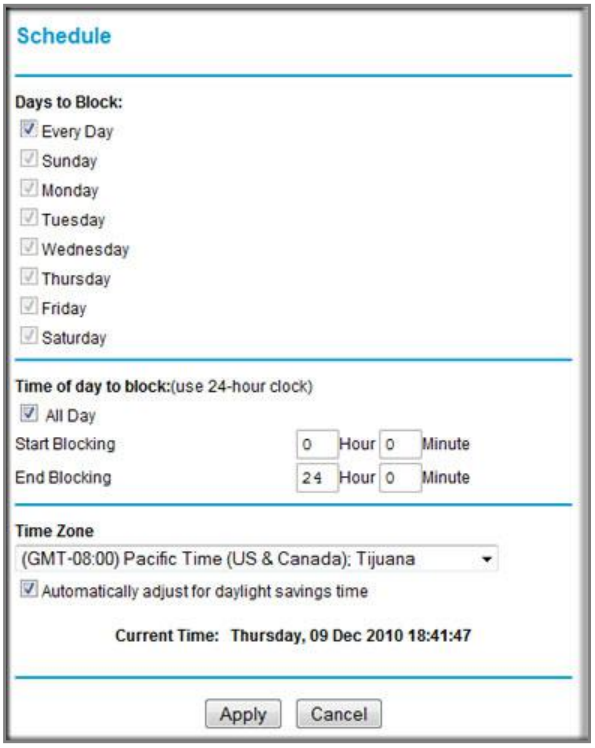



   - **Name**. Enter a meaningful name for the service.
   - **Type**. Select the correct type for this service. If in doubt, select **TCP/UDP**. The options are TCP, UDP, and TCP/UDP.
   - **Start Port** and **Finish Port**. If a port range is required, enter the range here. If a single port is required, enter the same value in both fields.
4. Click **Apply** to save your changes.

# Set the Time Zone

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

1. Select **Security > Schedule**.




2. Select your time zone. This setting determines the blocking schedule and time-stamping of log entries.
3. If your time zone is in daylight savings time, select the **Adjust for daylight savings time** check box to add one hour to standard time.

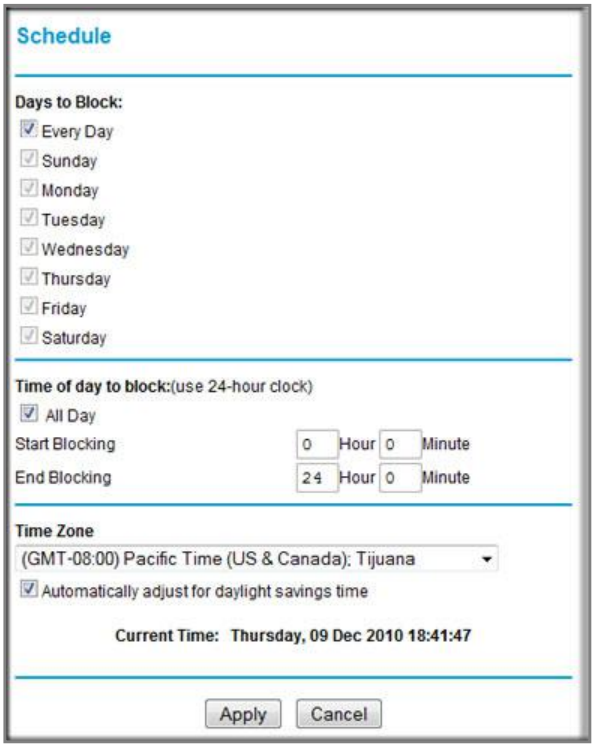
   ***Note:*** *If your region uses daylight savings time, select* ***Adjust for daylight savings time*** *on the first day and clear it after the last day.*

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

# Schedule Services

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

1. Select **Security > Schedule**.




2. To block Internet services based on a schedule, select **Every Day** or select one or more days.
3. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, enter times in the Start Blocking and End Blocking fields.

   ***Note:*** *Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule is effective through midnight the next day.*

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

# Enable Security Event Email Notification

To receive logs and alerts by email, provide your email information in the E-mail screen and specify which alerts you want to receive and how often.

Select **Security > E-mail** to display the following screen:

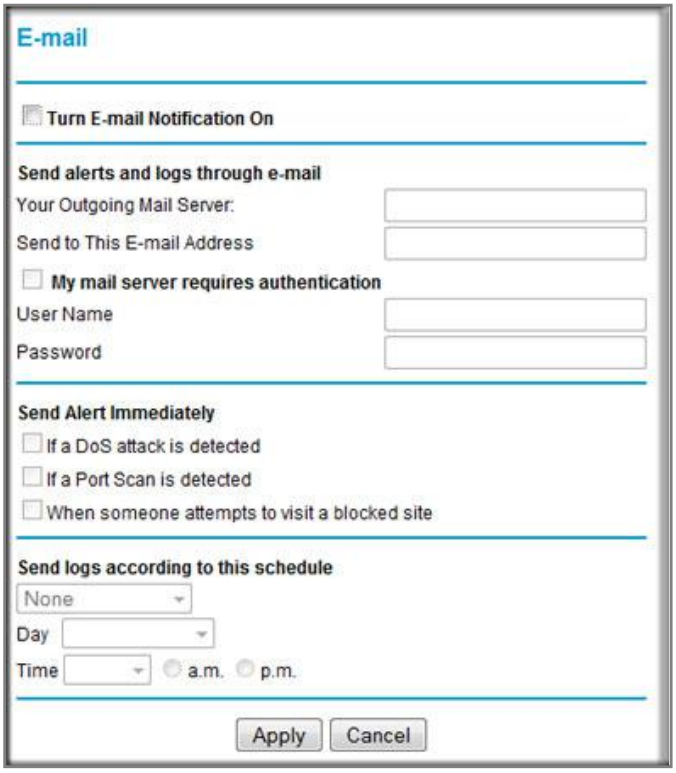



**Figure 12. E-Mail screen**

- **Turn E-mail Notification On**. Select this check box if you want to receive email logs and alerts from the modem router.
- **Send to This E-mail Address**. Enter the email address where you want logs and alerts sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.
- **Your Outgoing Mail Server**. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your email program. Enter the email address to which logs and alerts are sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.
- **My mail derver requires authentication**. If you use an outgoing mail server provided by your current ISP, you do not need to select this field. If you use an email account that is not provided by your ISP, select this field, and enter the required user name and password information.

- **Send Alerts Immediately**. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - **Days** specifies which day of the week to send the log. This is relevant when the log is sent weekly.
  - **Time** specifies the time of day to send the log. This is relevant when the log is sent daily or weekly.

**Note:** If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot email the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.

# Network Maintenance

# 5

## Administering your network

This chapter describes the modem router settings for administering and maintaining the modem router and home network.

This chapter contains the following sections:

# Upgrade the Modem Router Firmware

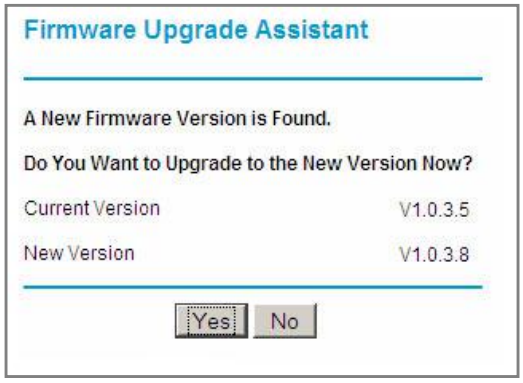
The modem router firmware (routing software) is stored in flash memory. By default, when you log in to your modem router, it checks the NETGEAR website for new firmware and alerts you if there is a newer version.

**WARNING!**

**When uploading firmware to the modem router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.**

## Automatic Firmware Check

When automatic firmware checking is on, the modem router performs the check and notifies you if an upgrade is available or not as shown here.





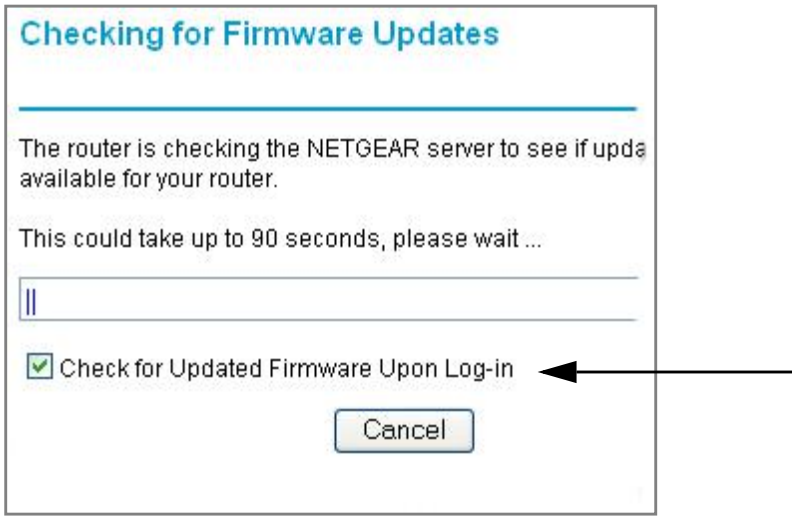
1. Click **Yes** to allow the modem router to download and install the new firmware. The upgrade process could take a few minutes. When the upload is complete, your modem router restarts.
2. Go to the DGN2200 support page at *http://www.netgear.com/support.*and read the new firmware release notes to determine whether you need to reconfigure the modem router after upgrading.

**Note:** If you get a “Firmware needs to be reloaded” message, it means a problem has been detected with the modem router’s firmware. Follow the prompts to correct the problem or see *Incorrect Date or Time* on page 136 for a description of the steps.

## Stop the Automatic Firmware Check

You can turn the automatic firmware checking off and check for firmware updates manually if you prefer. See *Manually Check for Firmware Upgrades* on page 55. To turn off the automatic firmware check at login:

1. Select **Maintenance > Router Upgrade**.
2. Clear the **Check for Updated Firmware Upon Log-in** check box.




# Manually Check for Firmware Upgrades

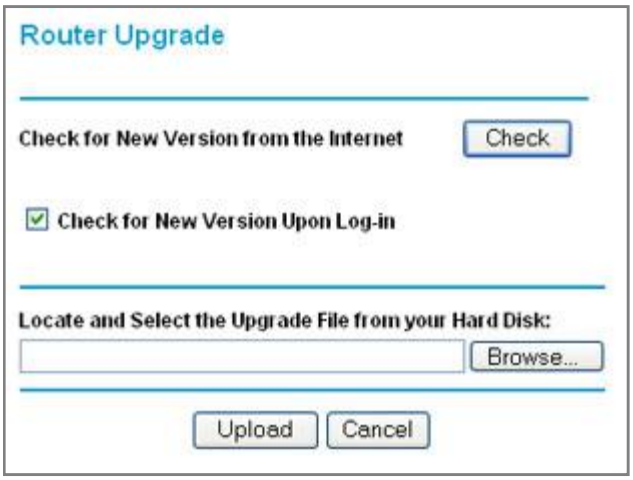
You can use the Router Upgrade screen to manually check the NETGEAR website for newer versions of firmware for your product.

**WARNING!**

**When uploading firmware to the modem router, *do not* interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.**

1. Select **Maintenance > Router Status** and make a note of the modem router firmware version number.
2. Go to the DGN2200 support page on the NETGEAR website at *http://www.netgear.com/support.*
3. If the firmware version on the NETGEAR website is newer than the firmware on your modem router, download the file to your computer.

4. Select **Maintenance > Router Upgrade** to display the following screen:




5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img).
6. Click **Upload** to send the firmware to the modem router.

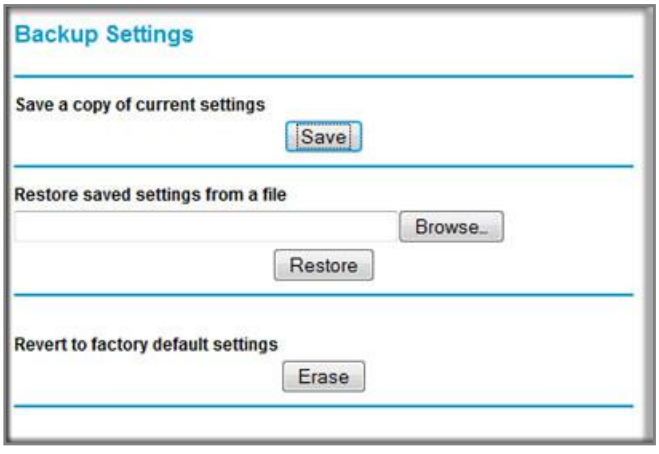
   When the upload is complete, your modem router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether or not you need to reconfigure the modem router after upgrading.

# Manage the Configuration File

The modem router configuration settings are stored in a configuration file (*.cfg). This file can be backed up to your computer, restored, or used to revert to factory default settings.

## Back Up

1. Select **Maintenance > Backup Settings** to display the following screen:




2. Click **Save** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

## Restore

1. Enter the full path to the file on your network, or click the **Browse** button to find the file.
2. When you have located the .cfg file, click the **Restore** button to upload the file to the modem router.

Upon completion, the modem router reboots.

## Erase

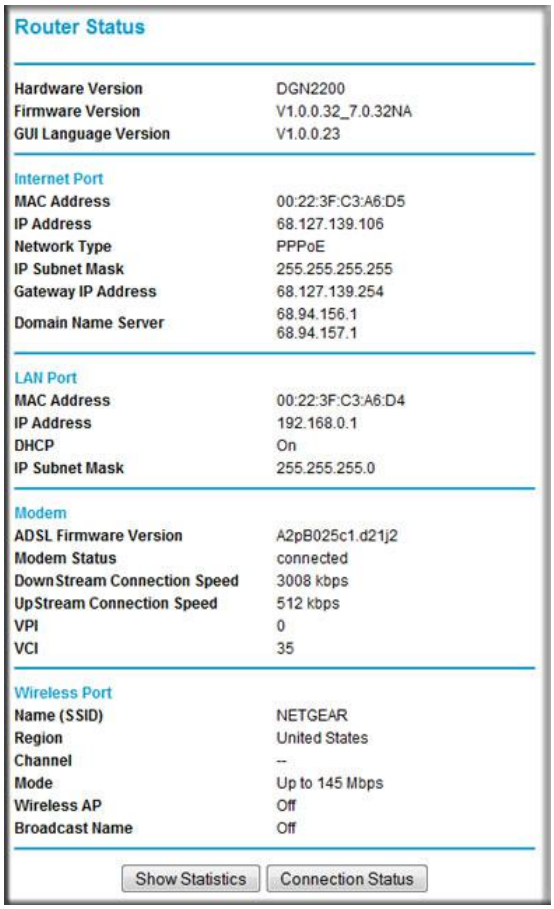
Click the **Erase** button to reset the modem router to its factory default settings. Erase sets the password to **password**, the LAN IP address to **192.168.0.1**, and enables the modem router's DHCP.

# View Router Status

Select **Maintenance > Router Status** to display this screen. The Router Status screen provides status and usage information.

**Hardware and Firmware Version**. The model of the hardware and the currently running firmware version.

**GUI Language Version**. The currently selected language.




## Internet Port Settings

**MAC Address**. The Ethernet MAC address of the DSL port.

**IP Address**. The DSL port IP address. If no address is shown, the modem router cannot connect to the Internet.

**Network Type**. The value depends on your ISP.

**IP Subnet Mask**. The DSL port IP subnet mask.

**Gateway IP Address**. The IP address used as a gateway to the Internet for computers configured to use DHCP.

**Domain Name Server**. The modem router DNS server IP addresses. These addresses are usually obtained dynamically from the ISP.

## LAN Port (Local Ports)

**MAC Address**. The modem router LAN port Ethernet MAC address.

**IP Address**. The modem router LAN port IP address. The default is 192.168.0.1.

**DHCP**. If Off, the modem router does not assign IP addresses to PCs on the LAN. If On, the modem router does assign IP addresses to PCs on the LAN.

**IP Subnet Mask**. The IP subnet mask used by the modem router LAN. The default is 255.255.255.0.

## Modem

**ADSL Firmware Version**. The version of the firmware.

**Modem Status**. The connection status of the modem.

**DownStream Connection Speed**. The modem receives data from the DSL line at this speed.

**UpStream Connection Speed**. The modem transmits data to the DSL line at this speed.

**VPI**. The Virtual Path Identifier setting.

**VCI**. The Virtual Channel Identifier setting.

## Wireless Port

See *Wireless Settings Screen* on page 33 for a more detailed description of these settings.

**Name (SSID)**. The Wi-Fi network name (service set ID) for the wireless network.

**Region**. The country where the unit is set up for use.

**Channel**. The current channel, which determines the operating frequency.

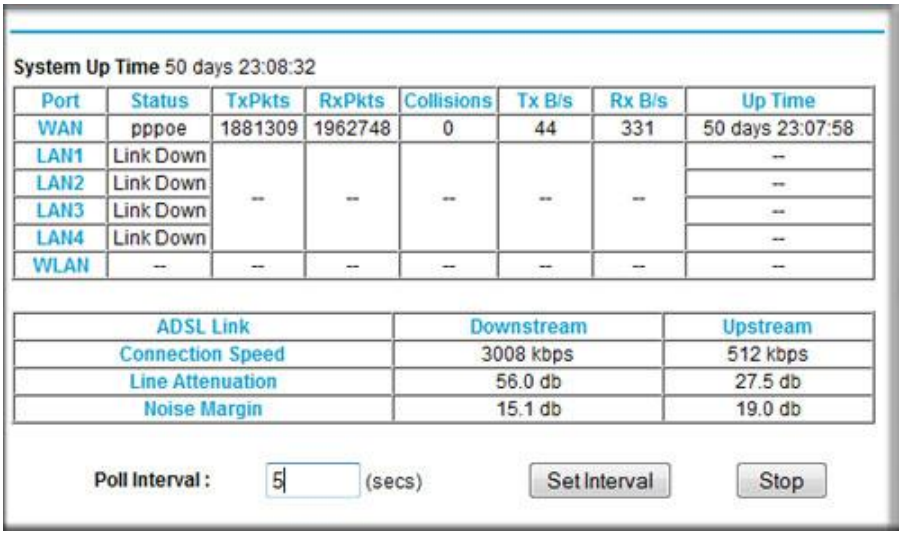
**Mode**. The current mbps setting.

**Wireless AP**. Indicates if the access point feature is enabled. If disabled, the Wireless LED on the front panel is off.

**Broadcast Name**. Indicates if the modem router is configured to broadcast its SSID.

# Show Statistics

Click the **Show Statistics** button on the Router Status screen to display a screen similar to this:



System Up Time 50 days 23:08:32

| Port | Status | TxPkts | RxPkts | Collisions | Tx B/s | Rx B/s | Up Time |
|---|---|---|---|---|---|---|---|
| WAN | pppoe | 1881309 | 1962748 | 0 | 44 | 331 | 50 days 23:07:58 |
| LAN1 | Link Down | -- | -- | -- | -- | -- | -- |
| LAN2 | Link Down | | | | | | -- |
| LAN3 | Link Down | | | | | | -- |
| LAN4 | Link Down | | | | | | -- |
| WLAN | -- | -- | -- | -- | -- | -- | -- |

| ADSL Link | Downstream | Upstream |
|---|---|---|
| Connection Speed | 3008 kbps | 512 kbps |
| Line Attenuation | 56.0 db | 27.5 db |
| Noise Margin | 15.1 db | 19.0 db |

Poll Interval : 5 (secs) Set Interval Stop

## *Port*

The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:

- **Status**. The link status of the port.
- **TxPkts**. The number of packets transmitted since reset or manual clear.
- **RxPkts**. The number of packets received since reset or manual clear.
- **Collisions**. The number of collisions since reset or manual clear.
- **Tx B/s**. The current line utilization—percentage of current bandwidth used.
- **Rx B/s**. The average line utilization.
- **Up Time**. The time elapsed since the last power cycle or reset.

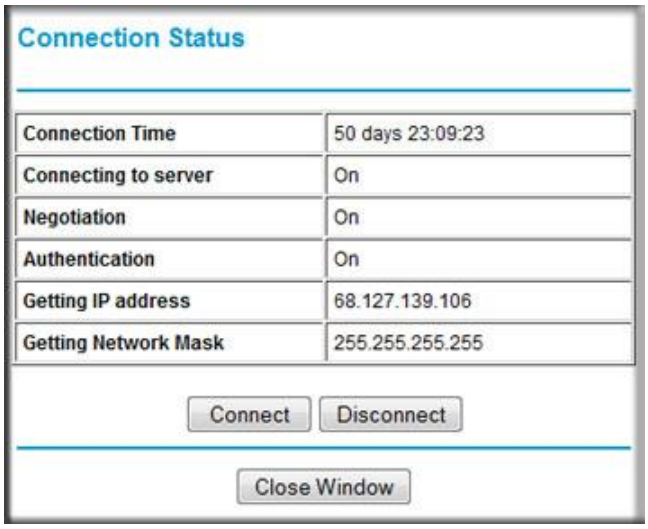
## *ADSL Link Downstream or Upstream*

The statistics for the upstream and downstream DSL link. These statistics are of interest to your technical support representative if you have problems obtaining or maintaining a connection.

- **Connection Speed**. Typically, the downstream speed is faster than the upstream speed.
- **Line Attenuation**. The line attenuation increases the farther you are physically located from your ISP's facilities.
- **Noise Margin**. The signal-to-noise ratio, which is a measure of the quality of the signal on the line.
- **Poll Interva**l. The interval at which the statistics are updated in this window. Click the **Stop** button to freeze the display.

## Connection Status

In the Router Status screen, click the **Connection Status** button to display a screen similar to this:




- **Connection Time**. The time elapsed since the last connection to the Internet through the DSL port.
- **Connecting to sender**. The connection status.
- **Negotiation**. On or Off.
- **Authentication**. On or Off.
- **Getting IP Address**. The IP address assigned to the WAN port by the ISP.
- **Getting Network Mask**. The network mask assigned to the WAN port by the ISP.

# View Attached Devices

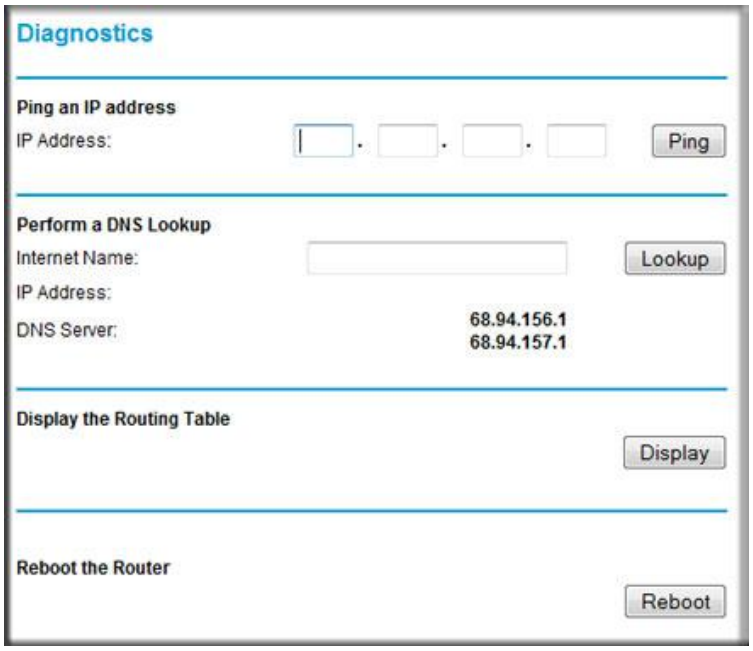
The Attached Devices screen shows all IP devices that the modem router has discovered on the local network.

Select **Maintenance > Attached Devices**.

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

# Run Diagnostic Utilities

The modem router has a diagnostics feature. Select **Maintenance > Diagnostics** to display the following screen.




You can perform the following functions:

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

# USB Storage

# 6

This chapter describes how to access and configure a USB storage drive attached to your modem router.

**Figure 13. USB port on rear panel.**

The USB port on the modem router can be used only to connect USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, printers, CD drives, or DVD drives to the this USB port.

This chapter includes the following sections:

# USB Drive Requirements

The modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown in the following table.

| Bus | Speed/Second |
|---|---|
| USB 1.1 | 12 Mbits |
| USB 2.0 | 480 Mbits |

Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables. The modem router should work with USB 2.0-compliant or 1.1-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the modem router, go to *http://kb.netgear.com/app/answers/detail/a_id/12345*.

When selecting a USB device, bear in mind the following:

- The USB port on the modem router can be used with one USB hard drive at a time. Do not attempt to use a USB hub attached to the USB port.
- According to the USB 2.0 specification, the maximum available power is 5V @ 0.5A. If a USB device exceeds this requirement, it might not function or might function erratically. Check the documentation for your USB device to be sure.
- The modem router supports FAT, FAT32, NTFS (read only), and NTFS with compression format enabled (read only).

# File-Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes.

## Share Photos within Your Home Network

You can create your own central storage location for photos and multimedia. This eliminates the need to log in to (and pay for) an external photo-sharing site.

1. Insert your USB drive into the USB port on the modem router either directly or with a USB cable.

   Computers on your local area network (LAN) can access this USB drive using a Web browser or Microsoft networking.

2. If you want to specify read-only access, or to allow access from the Internet, see *USB Storage Advanced Settings* on page 67.

## Share Large Files with FTP via Internet

1. To protect your network, set up security if someone else will be downloading the files. Create a user name and password with appropriate access.
2. If you want to limit USB drive access to only read access, from the modem router USB Storage (Basic Settings) screen, click **Edit a Network folder**. In the Write Access field, select **admin**, and then click **Apply**.

   The password for admin is the same one that you use to access the modem router. By default it is **password**.
3. Enable FTP via Internet in the USB Storage (Advanced Settings) screen. See *USB Storage Advanced Settings* on page 67.

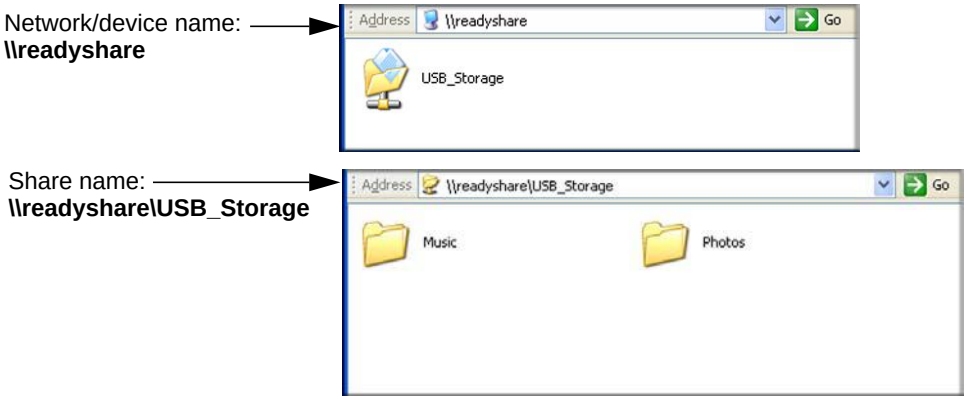
# USB Storage Basic Settings

You can view or edit basic settings for the USB storage device attached to your modem router.

1. Select **USB > Basic Settings**. The following screen displays:


   By default, the USB device is available to all computers on your local area network (LAN).
2. To access your USB device, do one of the following:
   - Click the network or device name.
   - Click the share name.

- Type **\\readyshare** in the address field of your Web browser.




If you logged in to the modem router before you connected your USB device, you might not see your USB device in the modem router screens until you log out and then log in again.

## Basic Settings Screen Fields and Buttons

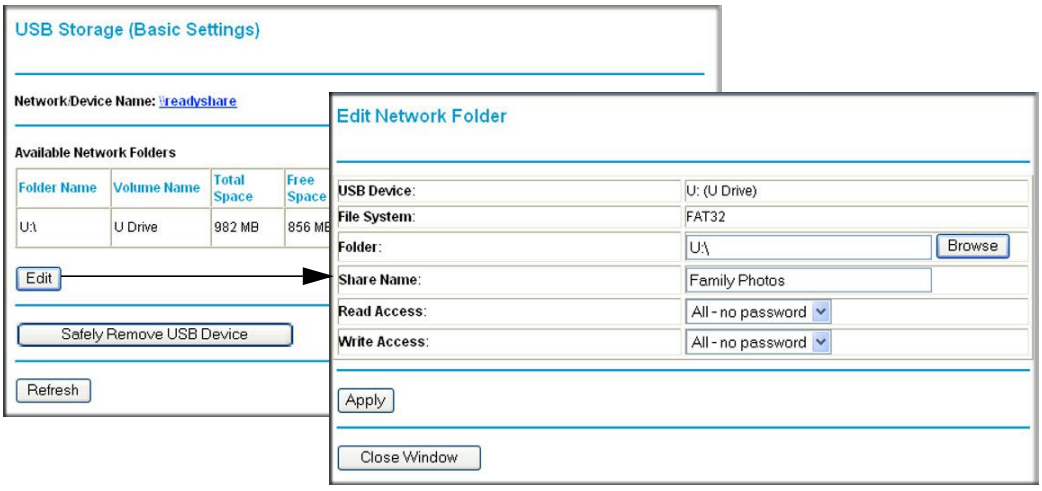
- **Network Device Name**. The default is \\readyshare. This is the name used to access the USB device connected to the modem router.
- **Folder Name**. Full path of the used by the Network folder.
- **Volume Name**. Volume name from the storage device (either USB drive or HDD).
- Total/Free Space. Shows the current utilization of the storage device.
- **Share Name**. You can click the name shown, or you can type it in the address field of your Web browser.

  If Not Shared is shown, then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
- **Read/Write Access**. Shows the network folder permissions and access controls.
  - All no password allows all users to access the network folder.
  - admin uses the same password that you use to log in to the modem router main menu.
- **Edit**. You can click the **Edit** button to edit the Available Network folder settings. See *Edit a Network Folder* on page 65.
- **Safely Remove USB Device**. Click this button to safely remove the USB device attached to your modem router. See *Unmount a USB Drive* on page 69.

# Edit a Network Folder

This process is the same from both the USB Storage (Basic Settings) and (Advanced Settings) screens.

1. Click the **Edit** button to open the Edit Network Folder screen:



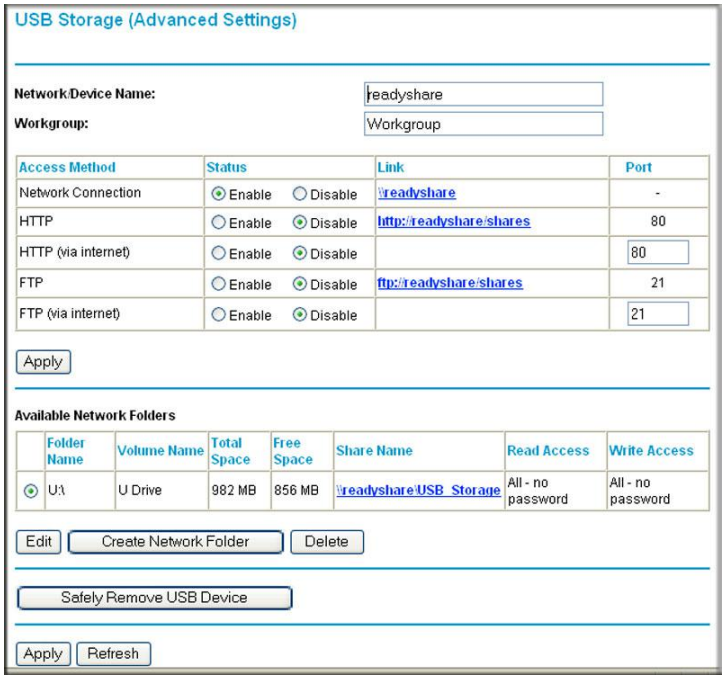

2. You can use this screen to select a folder, to change the share name, or to change read access or write access from All-no password to admin.

   The password for admin is the same one that is used to log in to the modem router main menu. By default it is password.

3. Click **Apply** for your changes to take effect.

# USB Storage Advanced Settings

To configure advanced USB settings, select **USB > Advanced Settings**. The USB Storage (Advanced Settings) screen displays:




You can use this screen to specify access to the USB storage device. The settings are as follows:

- **Network Device Name**. The default is readyshare. This is the name used to access the USB device connected to the modem router from your computer.
- **Workgroup**. If you are using a Windows Workgroup rather than a domain, the workgroup name is displayed here.

## *Access Method*

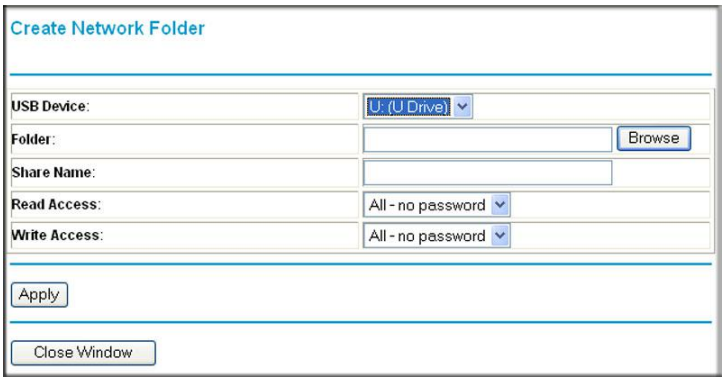
- **Network Connection**. Enabled by default, this allows all users on the LAN to have access to the USB drive.
- **HTTP**. Disabled by default. If you enable this setting, you can type **http://readyshare** to access the USB drive.
- **HTTP (via Internet)**. Disabled by default. If you enable this settings, remote users can type **http://readyshare** to access the USB drive over the Internet.
- **FTP**. Disabled by default.
- **FTP (via Internet)**. Disabled by default. If you enable this settings, remote users can access the USB drive via FTP over the Internet.

### *Available Network Folders*

- **Folder Name**. Full path of the Network folder.
- **Volume Name**. Volume name from the storage device (either USB drive or HDD).
- **Total Free Space**. The space currently available on the storage device.
- **Share Name**. You can click the name shown or you can type it into the address field of your Web browser. If Not Shared is shown, then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
- **Read/Write Access**. Shows the permissions and access controls on the Network folder. Selecting **All no password** allows all users to access the Network folder. You are prompted to enter the same password that you use to log in to the modem router.

## Create a Network Folder

1. From the USB Storage (Advanced Settings) screen, click the **Create Network Folder** button to open the Create a Network Folder screen:




2. Create a folder.
   - You can specify the folder's share name, read access, and write access from All-no password to admin.
   - The password for admin is the same one that is used to log in to the modem router main menu. By default it is password.
3. Click **Apply** so that your changes take effect.

# Unmount a USB Drive

To unmount a USB disk drive so that no users can access it, from the USB Settings screen, click the **Safely Remove USB** button. This takes the drive offline.

**CAUTION:**

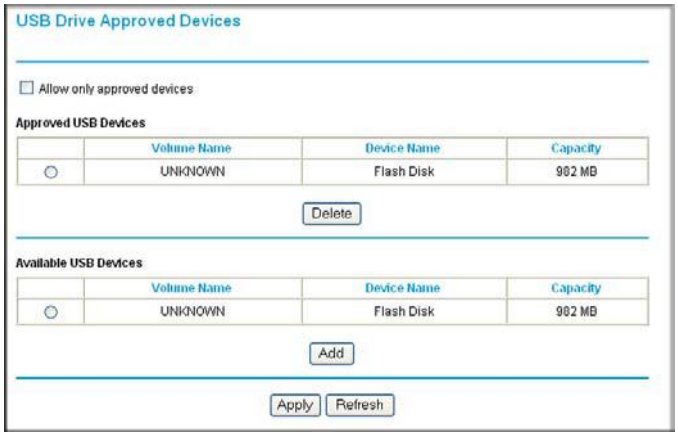
Unmount the USB drive before physically unplugging it from the modem router. If the USB disk is removed or a cable is pulled while data is being written to the disk, it could result in file or disk corruption.

# Approved USB Devices

You can specify which USB devices are approved for use when connected to the modem router.

1. Select **Advanced > USB Settings**.


2. Click **Approved Devices**.
3. On the USB Drive Approved Devices screen, select the USB device from the Available USB Devices list.
4. Click **Add**.
5. Select the **Allow only approved devices** check box.
6. Click **Apply** so that your change takes effect.




If you want to approve another USB device, you must first use the **Safely Remove USB Device** button to unmount the currently connected USB device. Connect the other USB device, and then repeat this process.

# Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers using a Web browser, you use the modem router's Internet port IP address.

## Locate the Internet Port IP Address

The Router Status screen shows the Internet port IP address:

1. Log in to the modem router.
2. Select **Maintenance > Router Status**.
3. Record the IP address that is listed for the Internet port. This is the IP address you can use to connect to the modem router remotely.

## Access the Modem Router's USB Drive Remotely with FTP

You can connect to the modem router's USB drive using a Web browser:

1. Connect to the modem router by typing **ftp://** and the Internet port IP address in the address field of Internet Explorer or Netscape Navigator, for example, **ftp://10.1.65.4**. If you are using Dynamic DNS, you can type the DNS name rather than the IP address.
2. Type the name and password of the account that has access rights to the USB drive.

   The directories of the USB drive that your account has access to display, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

# Connect to the USB Drive with Microsoft Network Settings

You can access the USB drive from local computers on your home or office network using Microsoft network settings. You must be running Microsoft Windows 2000, XP, or older versions of Windows with Microsoft networking enabled. You can use normal Explorer operations such as dragging and dropping, opening files, or cutting and pasting files from:

- Microsoft Windows Start menu, Run option
- Windows Explorer
- Network Neighborhood or My Network Place

## Enabling File and Printer Sharing

Each computer's network properties have to be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft networking have to be enabled, as described in the following sections.

**Note:** In Windows 2000 and Windows XP, File and Printer Sharing is enabled by default.

## *Configuring Windows 98SE and Windows ME*

The easiest way to get to your network properties is to go to your desktop, right-click **Network Neighborhood** and then select **Properties**. File and Printer Sharing for Microsoft Windows should be listed. If not, click **Add** and follow the installation prompts.

**Note:** If you have any questions about File and Printer Sharing, contact Microsoft for assistance.

## *Configuring Windows 2000 and Windows XP*

Right-click the network connection for your local area network. File and Printer Sharing for Microsoft Windows should be listed. If not, click **Install** and follow the installation prompts.

# Advanced Settings

# 7

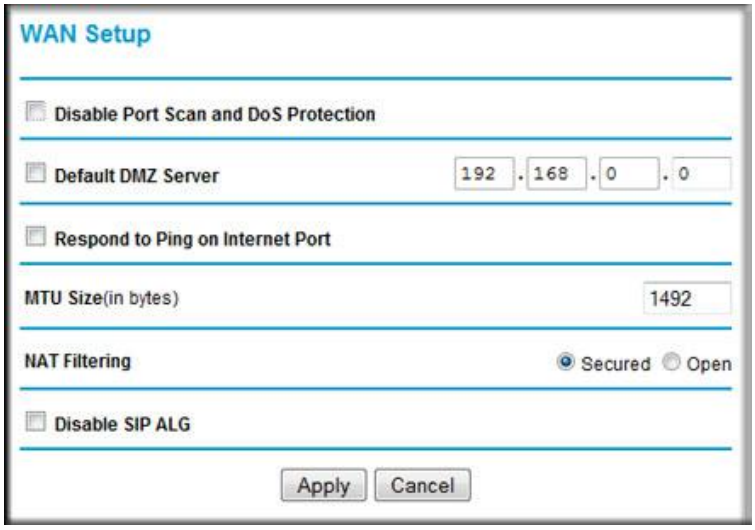
## Configuring for unique situations

This chapter describes the advanced features of your modem router. The information is for users with a solid understanding of networking concepts who want to set the modem router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter contains the following sections:

# WAN Setup

Select **Advanced > WAN Setup** to display the following screen:




The following settings are available:

- **Disable Port Scan and DoS Protection**. The firewall protects your LAN against port scans and denial of service (DoS) attacks. This protection should be disabled only in special circumstances.
- **Default DMZ Server**. The default demilitarized zone (DMZ) server feature is helpful when you use online games and video conferencing applications that are incompatible with NAT. See *Default DMZ Server* on page 74.
- **Respond to Ping on Internet WAN Port**. If you want the modem router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, because it allows your modem router to be discovered. Do not select this check box unless you have a specific reason to do so.
- **MTU Size (in bytes)**. The normal Maximum Transmit Unit (MTU) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **NAT Filtering**. By default NAT filtering is used.
- **Disabling the SIP ALG**. The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The Disable SIP ALG check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

# Default DMZ Server

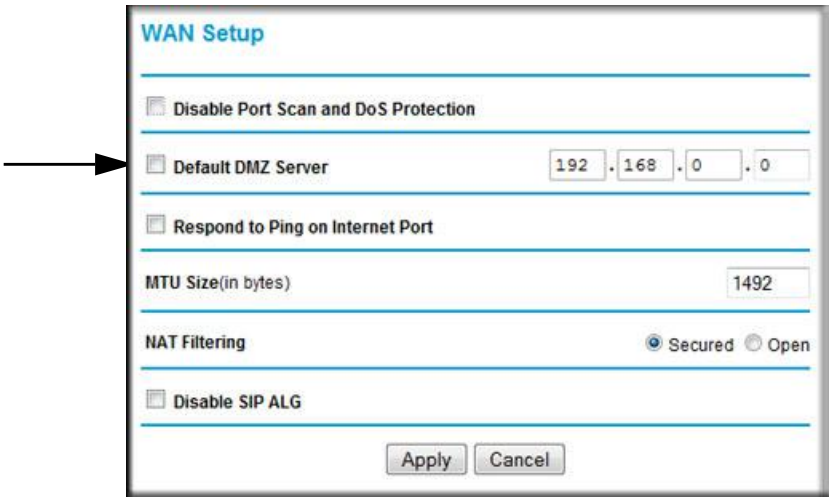
The default demilitarized zone (DMZ) server feature is helpful when you use online games and video conferencing applications that are incompatible with NAT. The modem router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

**Note:** For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall. If compromised via the Internet, the computer can be used to attack your network.

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

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

1. In the WAN Setup screen, select the **Default DMZ Server** check box.




2. Type the IP address for that server and click **Apply**.

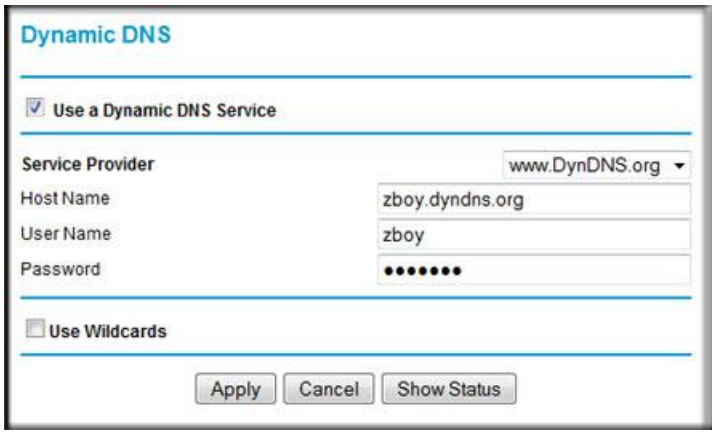
# Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name that is linked to your IP address by public Domain Name Servers (DNS). More commonly, Internet accounts have dynamically assigned IP addresses in which the IP addresses change frequently. In this case, use a commercial Dynamic DNS service to register your domain to its IP address and forward traffic directed at your domain to your current IP address.

The modem router has a client that can connect to a Dynamic DNS service provider. Once you set up Dynamic DNS in the modem router, when your IP address changes, your modem router contacts your Dynamic DNS service provider, logs in to your account, and registers your new IP address.

### To set up Dynamic DNS:

1. Select **Advanced > Dynamic DNS** to display the following screen.




2. Access the website of one of the Dynamic DNS service providers whose names appear in the Service Provider drop-down list, and register for an account. For example, for dyndns.org, go to www.dyndns.org.
3. Select the **Use a Dynamic DNS Service** check box.
4. Select the name of your Dynamic DNS service provider.
5. Type the host name that your Dynamic DNS service provider gave you. This is sometimes called the domain name. If your URL is myName.dyndns.org, your host name is myName.
6. Type the user name for your Dynamic DNS account.
7. Type the password (or key) for your Dynamic DNS account.
8. 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 causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
9. Click **Apply** to save your settings.

If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the Dynamic DNS service does not work because private addresses are not routed on the Internet.

# LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as DHCP and Routing Information Protocol (RIP). The modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The modem router's default LAN IP configuration is as follows:

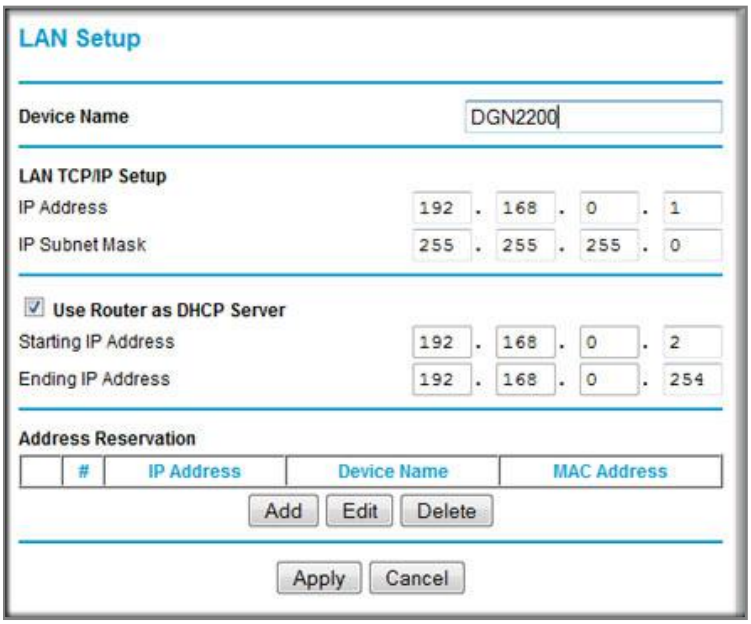
- **LAN IP address**. 192.168.0.1
- **Subnet mask**. 255.255.255.0

These addresses are part of the private address range designated by the Internet Engineering Task Force (IETF *http://www.ietf.org/*) for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in the LAN Setup screen.

**Note:** If you change the LAN IP address of the modem router while connected through the browser, you are disconnected. To reconnect, open a new connection to the new IP address and log in.

### To change the LAN settings:

1. Select **Advanced > LAN Setup**.




2. Enter the LAN Setup configuration and click **Apply** to save your changes.

## LAN Setup Screen Settings

- **IP Address**. The LAN IP address of the modem router.
- **IP Subnet Mask**. The LAN subnet mask of the modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or modem router.
- **Use Router as DHCP Server**. By default, the modem router is a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the modem router's LAN. The assigned default gateway address is the LAN address of the modem router. IP addresses are assigned to the attached PCs from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

  For most applications, the default DHCP and TCP/IP settings of the modem router are satisfactory.
- **Reserved IP Addresses Setup**. When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the modem router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

## IP Address Reservation

### To reserve an IP address:

1. Select **Advanced > LAN Setup** and click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. Choose an IP address from the modem router's LAN subnet, such as 192.168.0.x.
3. Type the MAC address of the computer or server.

   **Tip:** If the computer is already on your network, copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

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

### To edit or delete a reserved address entry:

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

# Quality of Service (QoS)

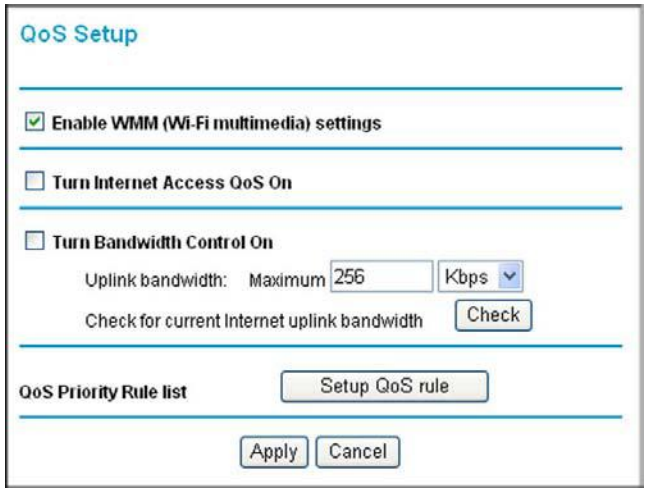
Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The modem router can provide QoS prioritization over the wireless link and on the Internet connection.

The modem router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application have to have WMM enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

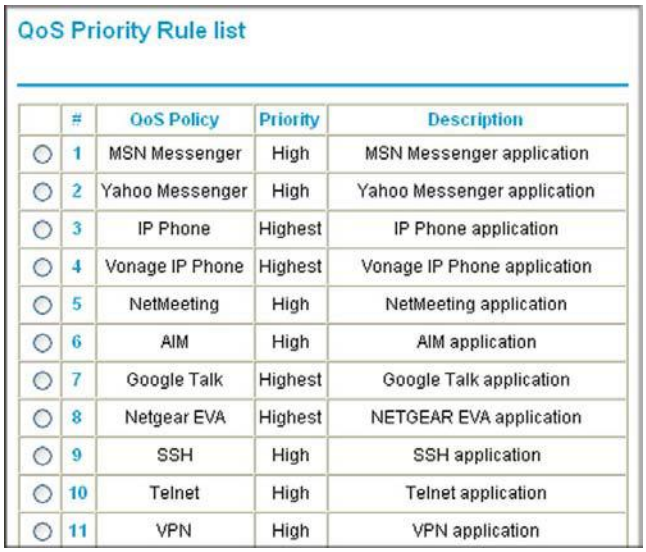
## QoS for Internet Access

To specify prioritization of traffic, you need to add or create a policy for the type of traffic.

1. Select **Advanced > QoS Setup**.



2. Click **Setup QoS rule**. The QoS Priority Rule list displays:

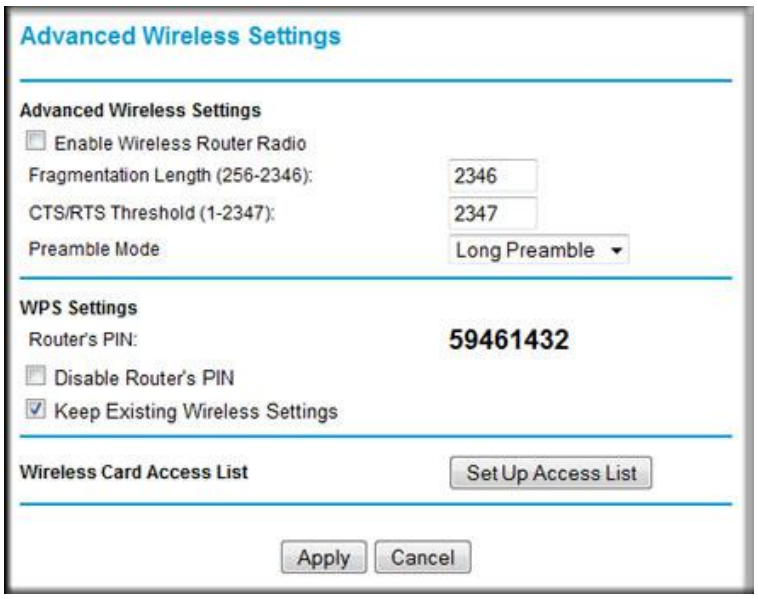



3. To change a rule, select its radio button, scroll down and click **Edit**.
4. To add a custom rule, click **Add Priority Rule**.
5. Click **Apply** to save your changes and return to the QoS Setup screen.
6. In the QoS Setup screen, click **Apply**.

# Advanced Wireless Settings

### To view or change advanced wireless settings:

1. Select **Advanced > Wireless Settings** to display the following screen:



**Note:** The advanced WPS settings section is not displayed if you selected WEP as the security option.

2. If you make changes, click **Apply**. Note that the WLAN settings come from the settings you made in the Wireless Settings screen (see *Wireless Settings Screen* on page 33).

## Advanced Wireless Settings

- **Enable Wireless Router Radio**. When this check box is selected, the modem router works as an access point broadcasting a wireless signal.
- **Fragmentation Length.**
- **CTS/RTS Threshold**.
- **Preamble Mode**.

## WPS Settings

**Router's PIN**. The PIN number that you use on a registrar (for example, from the Network Explorer on a Vista Windows PC) to configure the modem router's wireless settings through WPS. You can also find the PIN on the modem router label.

The PIN function might temporarily be disabled when the modem router detects suspicious attempts to break into the modem router's wireless settings by using the modem router's PIN through WPS. You can manually enable the PIN function by clearing the Disable Router's PIN check box.

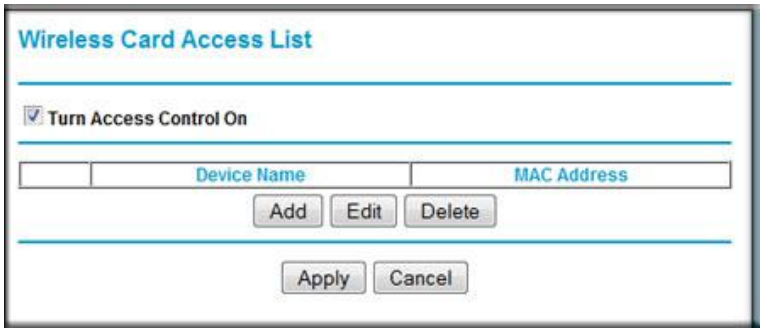
**Keep Existing Wireless Settings**. By default, the Keep Existing Wireless Settings check box is selected. This allows the modem router to keep the same SSID and wireless security settings when WPS-enabled devices are added to the network.

If the Keep Existing Wireless Settings check box is not selected, the next time you use WPS to connect WPS-capable devices to your wireless network, the modem router generates a new random SSID and WPA/WPA2 passphrase. NETGEAR does not recommend this.

# Wireless Card Access List

The Wireless Card Access List lets you restrict access to your network to a specific list of devices based on their MAC addresses. This section explains how to set up the list.

1. Select **Advanced > Wireless Settings**, and click the **Setup Access List** button to display the Wireless Card Access List screen:




   The Turn Access Control On check box is not selected so that any computer configured with the correct wireless network name (SSID) and passphrase to access the network.

2. Select the **Turn Access Control On** check box to enable access restriction by MAC address.
3. Click **Add** to add your computer's MAC address so that you do not lose your wireless connection when you click Apply. If you lose your wireless connection, you have to access the wireless modem router from a wired computer or from a wireless computer that is on the access control list. The following screen displays:

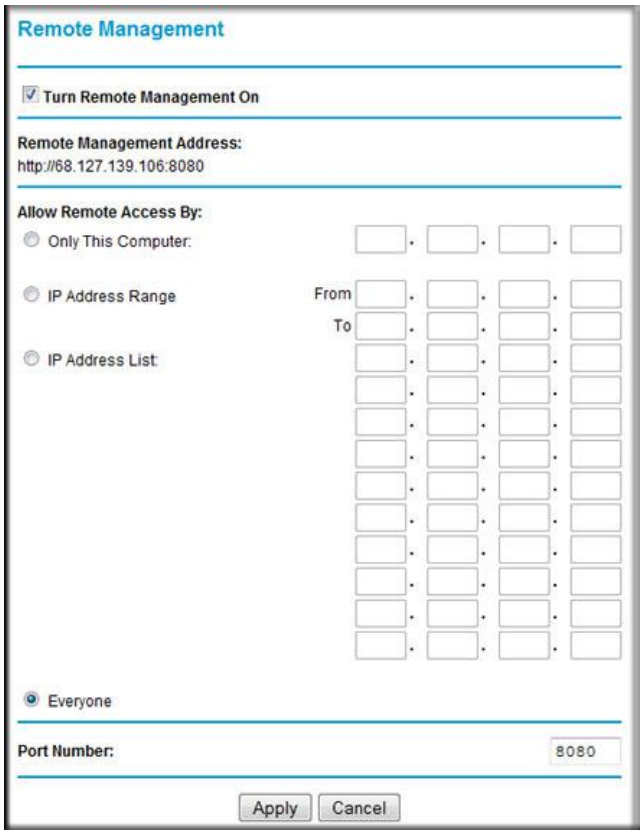

4. If a wireless station that you want to add is connected to the network, select it from the Available Wireless Cards list and click **Add**.
5. You can enter MAC addresses manually. The MAC address is usually printed on the wireless computer or device, or it might be in the modem router's DHCP table. The MAC address is 12 hexadecimal digits.

   You can copy and paste the MAC addresses from the modem router's Attached Devices screen (see *View Attached Devices* on page 60) into the MAC Address field. This screen shows computers connected to the network.

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

# Remote Management

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




1. Select **Advanced > Remote Management** to display this screen:
2. Select the **Turn Remote Management On** check box.
3. Specify the external addresses that can access remote management. For security, restrict access to as few external IP addresses as practical. Select a radio button:
   - **Only This Computer**. Allow access from a single IP address on the Internet.
   - **IP Address Range**. Allow access from a range of IP addresses on the Internet.
   - **IP Address List**. Enter each IP address that should have access.
   - **Everyone**. Allow access from any IP address on the Internet.
4. Specify the port number to be used for accessing the modem router interface.

   Web browser access usually uses the standard HTTP service port 80. For greater security, you can change it so the remote modem router interface uses a custom port by entering that number in the field provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
5. Click **Apply** to save your changes.

   To access your modem router from the Internet, type your modem router's WAN IP address in your browser's Address field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 at port number 8080, enter the following in your browser: **http://134.177.0.123:8080**.

**Note:** The http:// has to be included in the address.

# Static Routes

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

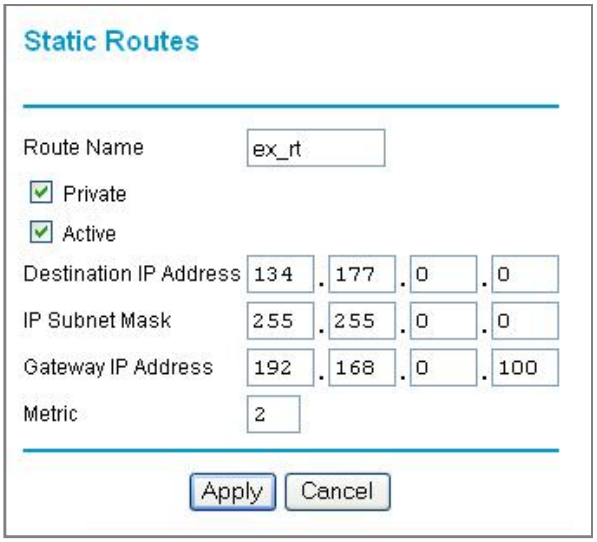
## Static Route Example

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 address is 134.177.0.0.

When you first configured your modem 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 modem router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you need to define a static route, telling your modem router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100.



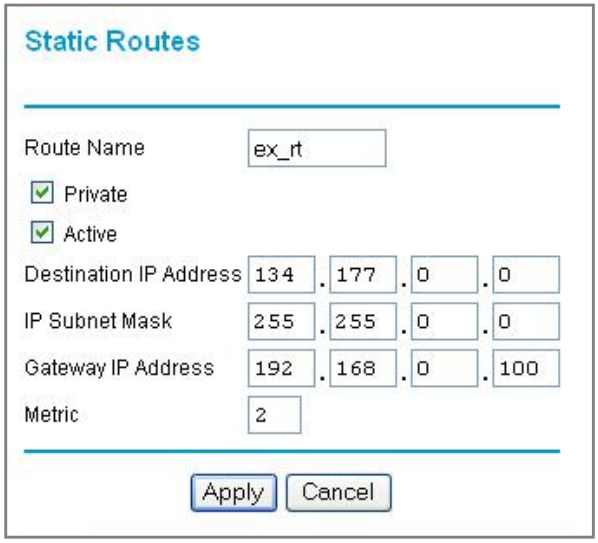

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses is to be forwarded to the ISDN router at 192.168.0.100.
- The value in the Metric field represents the number of routers between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.
- The Private check box is selected only as a precautionary security measure in case RIP is activated.

# Add a Static Route

1. Select **Advanced > Static Routes** to display the following screen:


2. Click **Add** to open the following screen.




3. Fill in the fields:
   - In the Route Name field, enter a route name for this static route. This name is for identification purpose only.
   - Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
   - Select **Active** to make this route effective.
   - Enter the destination IP address of the final destination.
   - Enter the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
   - Enter the gateway IP address, which has to be a router on the same LAN segment as the modem router.
   - In the Metric field, enter 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.
4. Click **Apply** to save your changes. The Static Routes table is updated to show the new entry.

# Universal Plug and Play

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

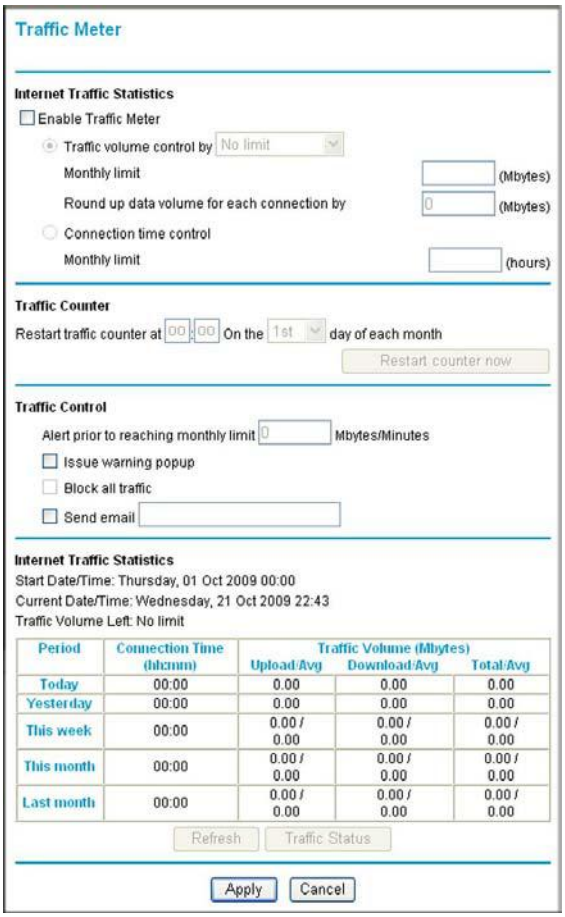
1. Select **Advanced > UPnP** to display the following screen:


2. Specify the settings as follows:
   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If UPnP is disabled, the modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the modem router.
   - **Advertisement Period**. The advertisement period is how often the modem router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time to Live**. This 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 is 4 hops, which works for most home networks. If you notice that some devices are not being updated or reached correctly, you might need to increase this value a little.
   - **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the modem router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.
3. To save, cancel your changes, or refresh the table:
   - Click **Apply** to save the new settings to the modem router.
   - Click **Cancel** to disregard any unsaved changes.
   - Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

# Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic passing through your modem router's Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

### To monitor traffic on your modem router:




1. Select **Advanced > Traffic Meter**.
2. To enable the Traffic Meter, select the **Enable Traffic Meter** check box.
3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:
   - **No limit**. No restriction is applied when the traffic limit is reached.
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both directions**. The restriction is applied to both incoming and outgoing traffic.
4. You can limit the amount of data traffic allowed per month:
   - By specifying how many Mbytes per month are allowed.
   - By specifying how many hours of traffic are allowed.
5. Set the Traffic Counter to begin at a specific time and date.
6. Set up Traffic Control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   - The Internet LED flashes green or amber.
   - The Internet connection is disconnected and disabled.
7. Set up Internet Traffic Statistics to monitor the data traffic.
8. Click the **Traffic Status** button if you want a live update on Internet traffic status on your modem router.
9. Click **Apply** to save your settings.

# Advanced USB Settings

For added security, you can specify that only approved USB devices are shared.

1. Select **Advanced > USB**. The following screen displays:


2. Select **No** and click **Apply**.
3. To define the approved devices, click **USB Approved Devices**.

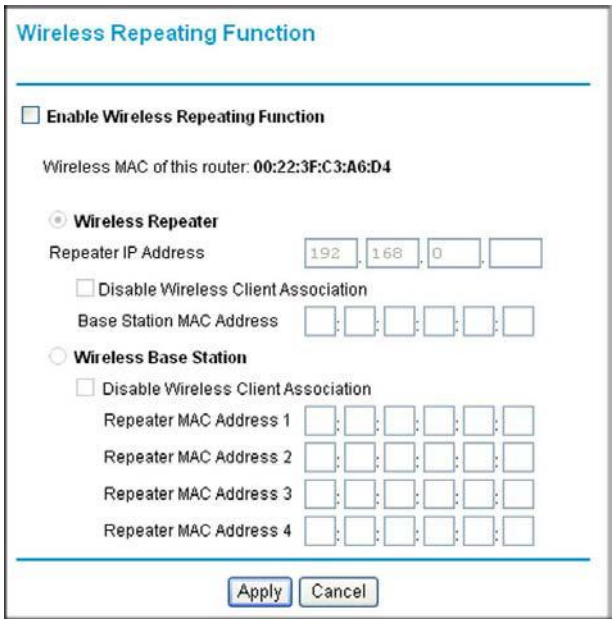
# Wireless Bridging and Repeating Networks

With the modem router, you can build large bridged wireless networks that form an IEEE 802.11n Wireless Distribution System (WDS). Using the modem router with other access points (APs) and wireless devices, you can connect clients using their MAC addresses rather than IP addresses. Here are some examples of wireless bridged configurations:

- **Point-to-point bridge**. The modem router communicates with another bridge-mode wireless station. See *Set Up a Point-to-Point Bridge* on page 89.
- **Multi-point bridge**. The modem router is the “master” for a group of bridge-mode wireless stations. Then all traffic is sent to this master, rather than to other access points. See *Set Up a Multi-Point Bridge* on page 90.
- **Repeater with wireless client association**. Sends all traffic to the remote access point. See *Repeater with Wireless Client Association* on page 91.

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

Select **Advanced > Wireless Repeating Function** to display the following screen:




- **Enable Wireless Repeating Function**. Select this check box if you want to use the wireless repeating function.
- **Wireless MAC of this router**. This field displays the MAC address for your modem router for your reference. You will need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.
- **Wireless Repeater**. If your modem router is the repeater, select this check box.
- **Repeater IP Address**. If your modem router is the repeater, enter the IP address of the other access point.
- **Disable Wireless Client Association**. If your modem router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.
  - If you are setting up a point-to-point bridge, select this check box.
  - If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.
- **Base Station MAC Address**. If your modem router is the repeater, enter the MAC address for the access point that is the base station.
- **Wireless Base Station**. If your modem router is the base station, select this check box.
- **Disable Wireless Client Association**. If your modem router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.
- **Repeater MAC Address (1 through 4)**. If your modem router is the base station, it can act as the “parent” of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

# Set Up a Point-to-Point Bridge

In point-to-point bridge mode, the modem router communicates as an access point with another bridge-mode wireless station. As a bridge, wireless client associations are disabled. Only wired clients can be connected. Use wireless security to protect this communication. The following figure shows an example of point-to-point bridge mode.

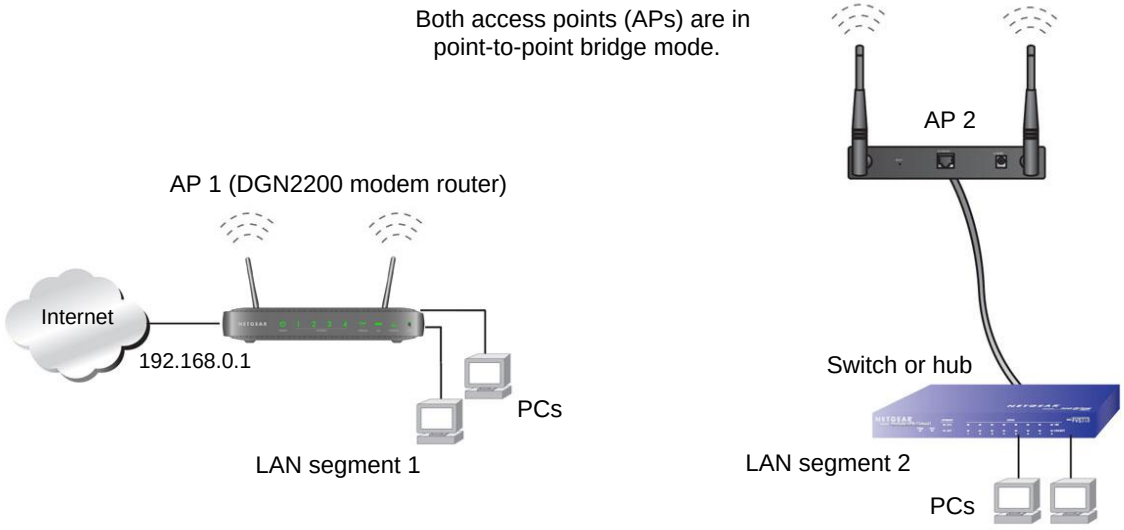



**Figure 14. Point-to-point bridge example**

### To set up a point-to-point bridge configuration:

1. Set up your modem router (AP 1) on LAN Segment 1 in point-to-point bridge mode.
   a. In the Wireless Repeating Function screen, select the **Enable Wireless Repeating Function** check box.
   b. Select either the **Wireless Repeater** or **Wireless Base Station** radio button.
   c. Select the corresponding **Disable Wireless Client Association** check box.
   d. Enter the MAC address for the other access point in the bridge. Depending on your selection in step a, use either the Base Station MAC Address field or the Repeater MAC Address 1 field.
   e. Click **Apply**.
2. Set up the other access point (AP 2) on LAN Segment 2 in point-to-point bridge mode.

   If your modem router is the repeater, then set up AP 2 as the base station; otherwise set up AP 2 as the repeater.
3. Set up both access points and verify that they use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.
4. Disable the DHCP server on AP 2. AP 1 will then be the DHCP server.
5. Verify connectivity across LAN Segment 1 and LAN Segment 2. A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

# Set Up a Multi-Point Bridge

Multi-point bridge mode allows a router to bridge to multiple peer access points simultaneously. Wireless client associations are disabled. Only wired clients can be connected. Multi-point bridge mode configuration includes the following steps:

- Set up the modem router for wireless repeating as the base station, and specify the MAC addresses of the access points that are repeaters.
- Set up the other access points for wireless repeating as repeaters, and specify the MAC address of the modem router as the base station.
- Use wireless security to protect this traffic.

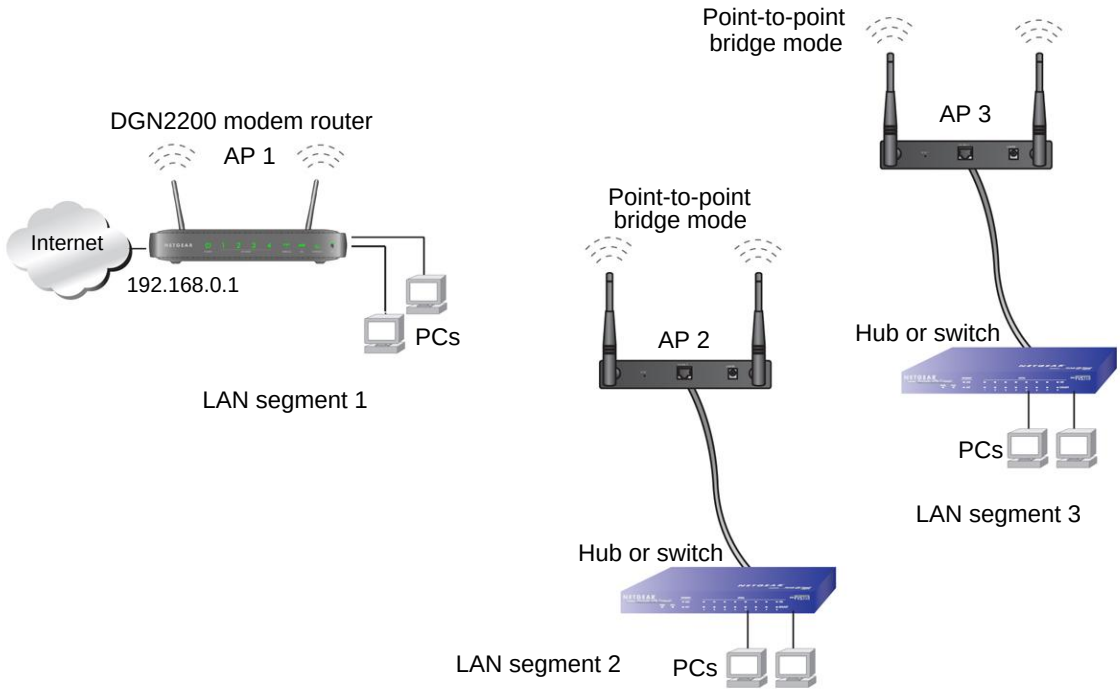



**Figure 15. Multi-point bridge example**

### To set up the multi-point bridge configuration:

In this example, the modem router is AP 1 on LAN Segment 1 because it is in a central location.

1. Set up your modem router to be the base station in the bridge.
   a. In the Wireless Repeating Function screen for your modem router, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Base Station** radio button.
   c. Select the corresponding **Disable Wireless Client Association** check box.
   d. Enter the MAC address for the other access points in the bridge in the Repeater MAC Address 1 and Repeater MAC Address 2 fields.
   e. Click **Apply**.

2. Set up AP 2 and AP 3 to be wireless repeaters.
   a. In the Wireless Repeating Function screen for AP 2 and AP 3, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Repeater** radio button.
   c. Select the corresponding **Disable Wireless Client Association** check box.
   d. Enter the MAC addresses for your modem router in the Base Station MAC Address field.
   e. Click **Apply**.
3. Disable the DHCP server on AP 2 and AP 3. AP 1 will then be the DHCP server.
4. Verify the following for all access points:
   - The modem router and other access points operate in the same LAN network address range as the LAN devices.
   - Only one access point, your modem router in **Figure 15**, is set up as the base station. The others are set up as repeaters.
   - All access points, including your modem router, are on the same LAN. That is, all the access point LAN IP addresses are in the same network.
   - If you are using DHCP, all access points should be set as DHCP clients. This setting is **Obtain an IP address automatically (DHCP Client)** in the Basic Settings screen.
   - All access points, including your modem router, use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.
5. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.

**Note:** Wireless stations configured as in *Figure 14* on page 89 cannot connect to the modem router or access points. If you want wireless stations to access any LAN segment, use additional access points in in any LAN segment.

## Repeater with Wireless Client Association

In the repeater mode with wireless client association, your modem router sends all traffic to a base station access point. You can set up the modem router as either the base station (parent) or as the repeater (child) access point.

Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this modem router.
- You cannot configure a sequence of parent-child APs. You are limited to only one parent access point, although if your modem router is the parent access point, it can connect with up to four child access points.

The following figure shows an example of a repeater mode configuration.

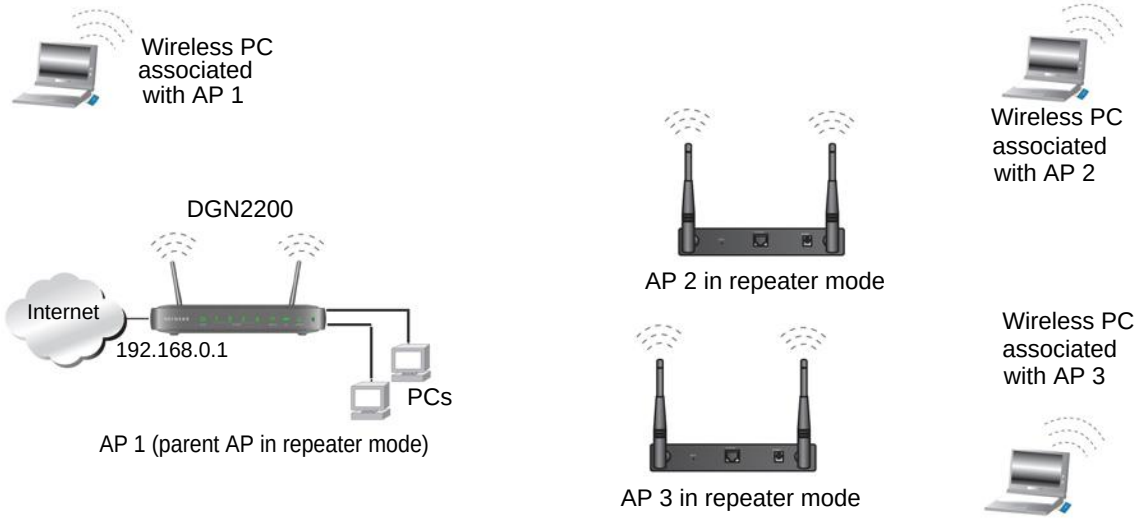



**Figure 16. Repeater example**

### To set up a repeater with wireless client association:

In this example, the modem router is the base station, but you can set it up to be the repeater with another AP as the base station if you want.

1. Set up your modem router to be the base station.
   a. In the Wireless Repeating Function screen for your modem router, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Base Station** radio button.
   c. Clear the corresponding **Disable Wireless Client Association** check box (make sure it is not selected).
   d. Enter the MAC addresses for AP 2 and AP 3 in the Repeater MAC Address 1 and Repeater MAC Address 2 field.
   e. Click **Apply**.
2. Set up AP 2 and AP 3 to be wireless repeaters.
   a. In the Wireless Repeating Function screen for AP 2 and AP 3, select the **Enable Wireless Repeating Function** check box.
   b. Select the **Wireless Repeater** radio button.
   c. Clear the corresponding **Disable Wireless Client Association** check box (make sure it is not selected).
   d. Enter the MAC addresses for your modem router in the Base Station MAC Address field.
   e. Click **Apply**.
3. Verify the following for all access points:
   - Each access point operates in the same LAN network address range as the LAN devices.

- The access points are on the same LAN. That is, the LAN IP addresses for the access points are in the same network.
- If you are using DHCP, access point devices are set to **Obtain an IP address automatically (DHCP Client)** in the Basic Settings screen.
- Access point devices use the same SSID, channel, authentication mode, and encryption.

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.

# Virtual Private Networking

# 8

This chapter describes how to use the virtual private networking (VPN) features of the modem router. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer. See *Appendix B, NETGEAR VPN Configuration*, and click the link to *Virtual Private Networking (VPN)* on page 159 to learn more about VPNs.

This chapter is organized as follows:

# Overview of VPN Configuration

Two common scenarios for VPN tunnels are between a remote PC and a network gateway; and between two or more network gateways. The DGN2200 supports both types. The DGN2200 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.

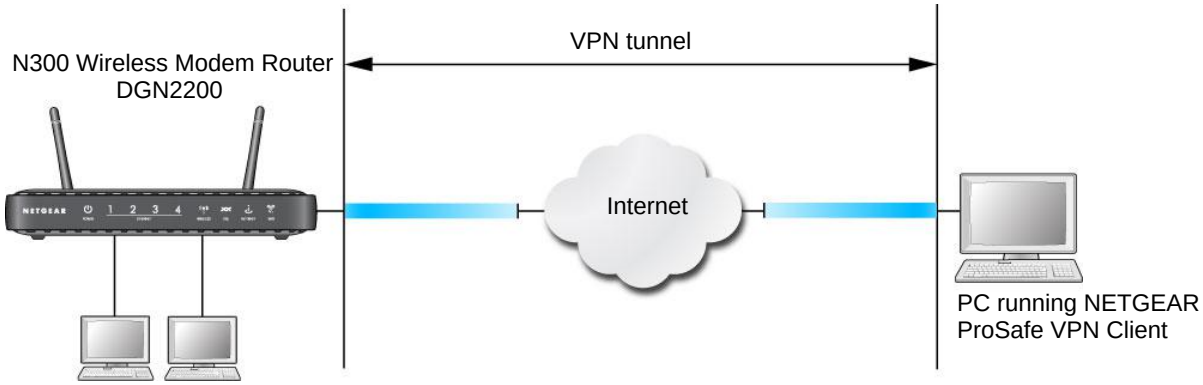



**Figure 17. Telecommuter VPN tunnel**

A VPN client access allows a remote PC to connect to your network from any location on the Internet. The remote PC is one tunnel endpoint, running the VPN client software. The modem router on your network is the other tunnel endpoint. (See *Set Up a Client-to-Gateway VPN Configuration* on page 98.)

## 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.

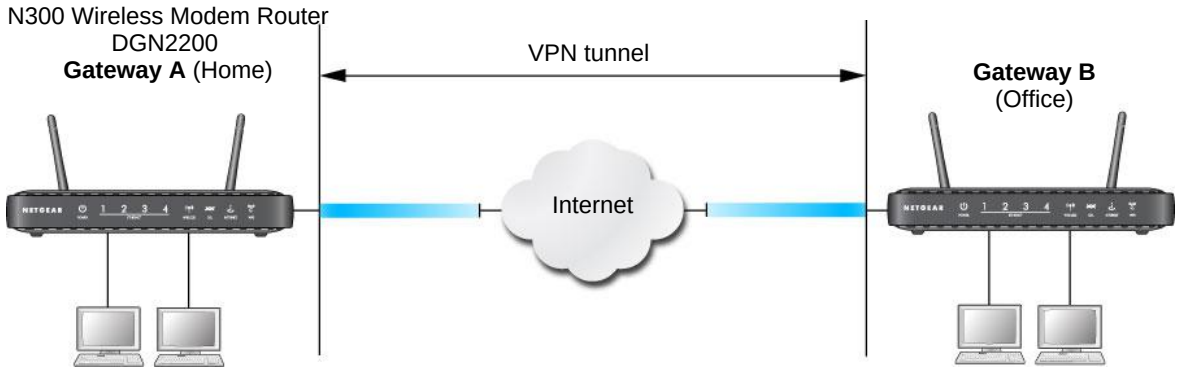



**Figure 18. VPN tunnel between networks**

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 gateways on each end of the tunnel to form the VPN tunnel end points. See *Set Up a Gateway-to-Gateway VPN Configuration* on page 108 for information about how to set up this configuration.

# Plan 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 3. VPN Tunnel Configuration Worksheet**

| **Parameter** | | **Value to Be Entered** | **Field Selection** | |
|---|---|---|---|---|
| Connection Name | | | N/A | |
| Pre-Shared Key | | | N/A | |
| Secure Association | | N/A | Main Mode | Manual Keys |
| Perfect Forward secrecy | | N/A | Enabled | Disabled |
| Encryption Protocol | | N/A | DES | 3DES |
| Authentication Protocol | | N/A | MD5 | SHA-1 |
| Diffie-Hellman (DH) Group | | N/A | Group 1 | Group 2 |
| Key Life in seconds | | | N/A | |
| IKE Life Time in seconds | | | N/A | |
| **VPN Endpoint** | **Local IPSecID** | **LAN IP Address** | **Subnet Mask** | **FQDN or Gateway IP (WAN IP Address** |
| | | | | |
| | | | | |

To set up a VPN connection, you need to configure each endpoint with specific identification and connection information describing the other endpoint. You 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 have to make a few choices first:

- Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will either endpoint use fully qualified domain names (FQDNs)? FQDNs supplied by Dynamic DNS providers (see *Using a Fully Qualified Domain Name (FQDN)* on

page 146) 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 has to always be the initiator.

- Which method will you use to configure your VPN tunnels?
  - The VPN Wizard using VPNC defaults (see *Table 4, Parameters Recommended by the BPNC and Used in the VPN Wizard* on page 97).
  - The typical automated Internet Key Exchange (IKE) setup (see *Use Auto Policy to Configure VPN Tunnels* on page 118).
  - A manual keying setup in which you need to specify each phase of the connection (see *Use Manual Policy to Configure VPN Tunnels* on page 125)?

**Table 4. Parameters Recommended by the BPNC and Used in the VPN Wizard**

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

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

# VPN Tunnel Configuration

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

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
  - See *Set Up a Client-to-Gateway VPN Configuration* on page 98.
  - See *Set Up a Gateway-to-Gateway VPN Configuration* on page 108.
- See *Use Auto Policy to Configure VPN Tunnels* on page 118 when the VPN Wizard and its VPNC defaults are not appropriate for your special circumstances, but you want to automate the Internet Key Exchange (IKE) setup.

- See *Use Manual Policy to Configure VPN Tunnels* on page 125 when the VPN Wizard and its VPNC defaults are not appropriate for your special circumstances and you have to 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 DGN2200 and the corresponding VPN endpoint gateway or client workstation.

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

# Set Up a Client-to-Gateway VPN Configuration

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

- *Step 1: Configure the Client-to-Gateway VPN Tunnel* on page 98 describes how to use the VPN Wizard to configure the VPN tunnel between the remote PC and network gateway.
- *Step 2: Configure the NETGEAR ProSafe VPN Client* on page 101 shows how to configure the NETGEAR ProSafe VPN Client endpoint.

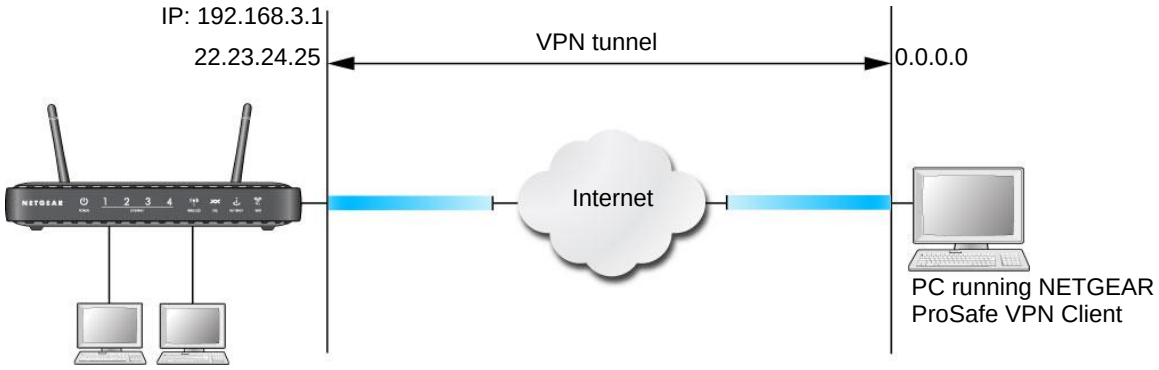



**Figure 19. Client-to-gateway VPN tunnel**

## Step 1: Configure the Client-to-Gateway VPN Tunnel

This section describes using the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in *Table 4* on page 97. If you have special requirements not covered by these VPNC-recommended parameters, see *Set Up VPN Tunnels in Special Circumstances* on page 118 for information about how to set up the VPN tunnel.

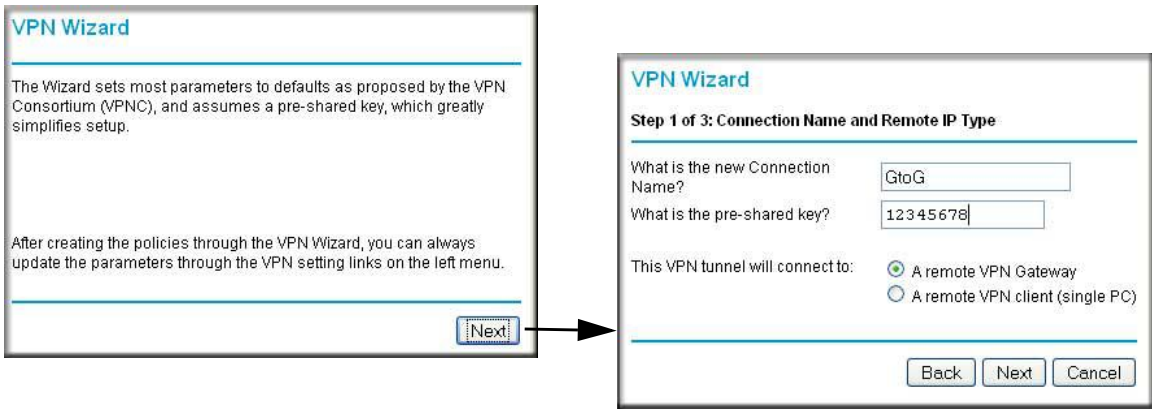
The following worksheet identifies the parameters used in this procedure, which are highlighted in blue. For a blank worksheet, see *Plan a VPN* on page 96.

**Table 5. VPN Tunnel Configuration Worksheet**

| Parameter | | Value to Be Entered | Field Selection | |
|---|---|---|---|---|
| Connection Name | | RoadWarrior | N/A | |
| Pre-Shared Key | | 12345678 | N/A | |
| Secure Association | | N/A | Main Mode | Manual Keys |
| Perfect Forward secrecy | | N/A | Enabled | Disabled |
| Encryption Protocol | | N/A | DES | 3DES |
| Authentication Protocol | | N/A | MD5 | SHA-1 |
| Diffie-Hellman (DH) Group | | N/A | Group 1 | Group 2 |
| Key Life in seconds | | 28800 (8 hours) | N/A | |
| IKE Life Time in seconds | | 3600 (1 hour) | N/A | |
| **VPN Endpoint** | **Local IPSecID** | **LAN IP Address** | **Subnet Mask** | **FQDN or Gateway IP (WAN IP Address)** |
| Client | toGateway | N/A | N/A | Dynamic |
| Gateway | toClient | 192.168.3.1 | 255.255.255.0 | 22.23.24.25 |

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

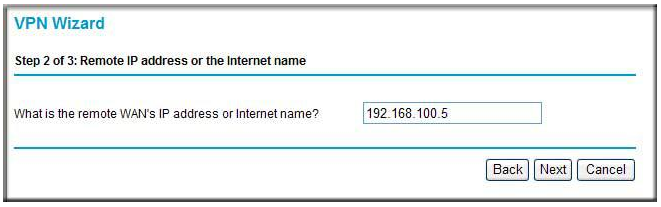
1. Select **Advanced - VPN > VPN Wizard**. The following screen displays. Click **Next**.



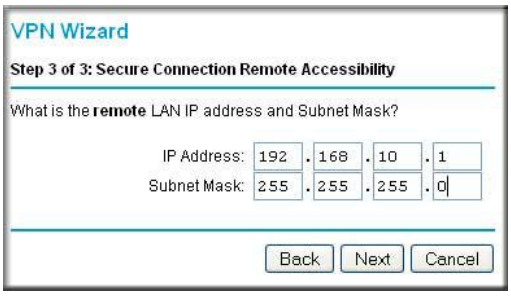

2. Fill in the Connection Name and pre-shared key fields.

   The connection name is for convenience and does not affect how the VPN tunnel functions.

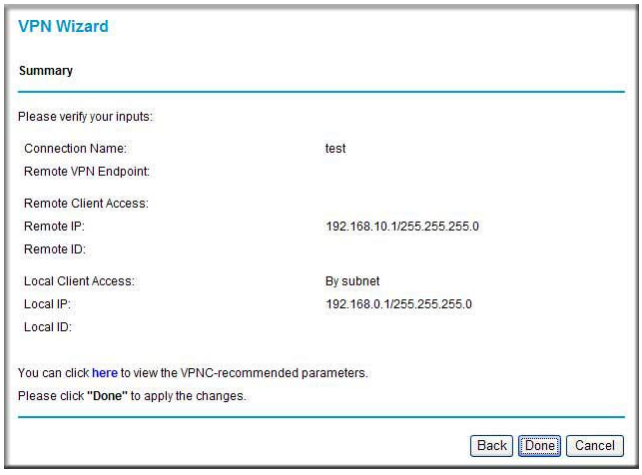
3. Select the radio button for the type of target end point, and click **Next**.




4. Enter the remote IP address and subnet mask, and click **Next**.

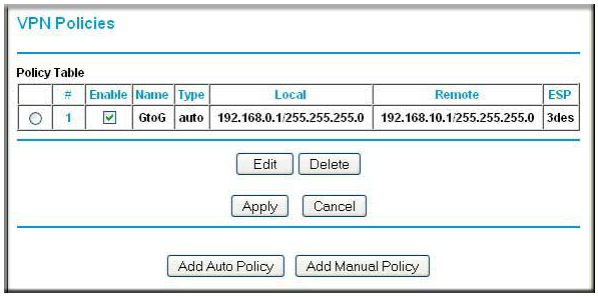



The Summary screen displays:




***Note:*** *To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the* ***here*** *link.*

5. Click **Done**. The VPN Policies screen displays, showing that the new tunnel is enabled:



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

> ***Note:*** *See Use Auto Policy to Configure VPN Tunnels on page 118 for information about how to enable the IKE keep-alive capability on an existing VPN tunnel.*

## Step 2: Configure the NETGEAR ProSafe VPN Client

This section describes how to configure the NETGEAR ProSafe VPN Client on a remote PC. These instructions assume that the PC running the client has a dynamically assigned IP address.

The PC has to have the NETGEAR ProSafe VPN Client program installed that supports IPSec. Go to the NETGEAR website (*http://www.netgear.com*) for information about how to purchase the NETGEAR ProSafe VPN Client.

> **Note:** Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you might be running on your PC. You might need to insert your Windows CD to complete the installation.

1. Install the NETGEAR ProSafe VPN Client on the remote PC, and then reboot.
   a. Install the IPSec component. You might have the option to install either the VPN adapter or the IPSec component or both. The VPN adapter is not necessary.

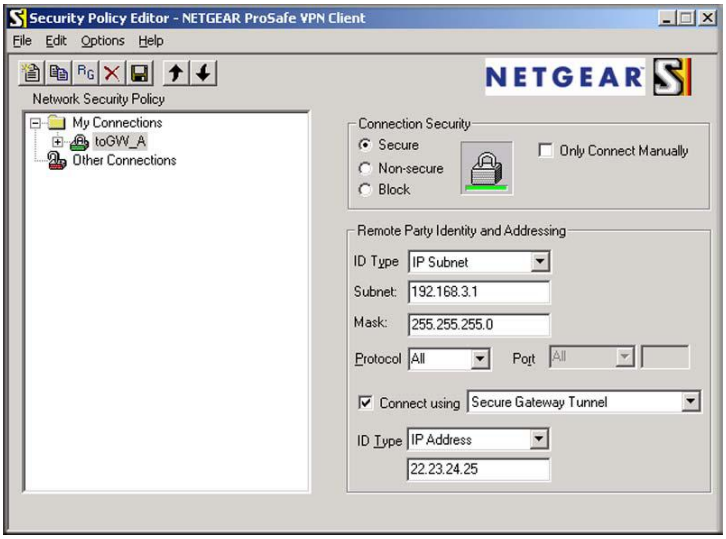
      If you do not have a modem or dial-up adapter installed in your PC, you might see the warning message stating “The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed.” You can disregard this message.

   b. Reboot the remote PC.

      The ProSafe icon (  ) is in the system tray.

   c. Double-click the ProSafe icon to open the Security Policy Editor.
2. Add a new connection.
   a. Run the NETGEAR ProSafe Security Policy Editor program, and, using the *Table 5* on page 99, create a VPN connection.

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




A New Connection listing appears in the list of policies.

**c.** Rename the new connection so that it matches the Connection Name field in the VPN Settings screen of the modem router on LAN A. Choose connection names that make sense to the people using and administering the VPN.

**Note:** In this example, the connection name used on the client side of the VPN tunnel is toGW_A, and it does not have to match the RoadWarrior connection name used on the gateway side of the VPN tunnel because connection names are irrelevant to how the VPN tunnel functions.

**d.** Enter the following settings:

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

**e.** Select **Connect using** and then select the **Secure Gateway Tunnel** check box.

**f.** In the ID Type drop-down list, select **IP Address**.

**g.** I the field directly below the ID Type drop-down list, enter the public WAN IP address of the modem router. In this example, 22.23.24.25 is used.

The resulting connection settings are shown in *Figure 20* on page 103.

3. Configure the security policy in the NETGEAR ProSafe VPN Client software:

   a. In the Network Security Policy list, expand the new connection by double-clicking its name or clicking the + symbol. My Identity and Security Policy subheadings appear below the connection name.

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

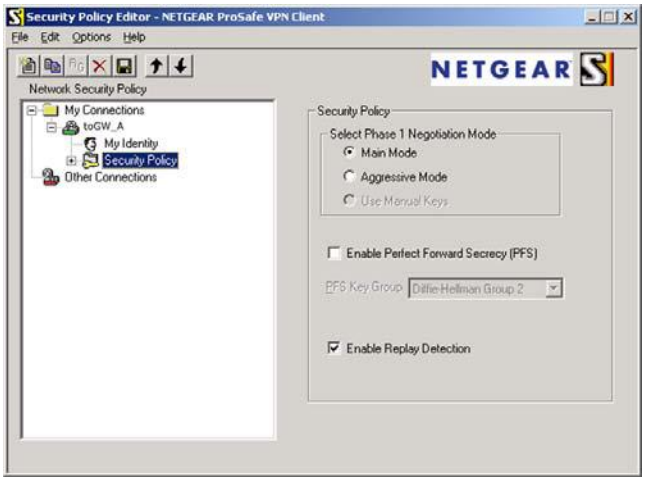


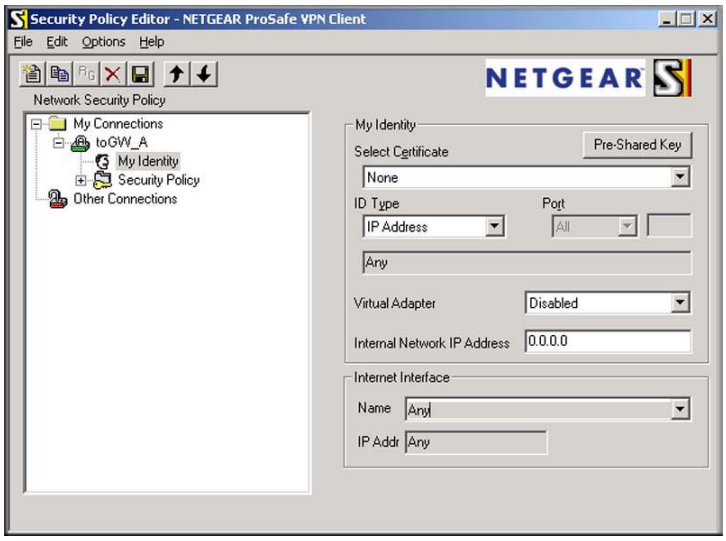

**Figure 20. Security Policy settings, Client-to-Gateway A**

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

4. Configure the VPN client identity.

   In this step, you provide information about the remote VPN client PC. You need to provide the pre-shared key that you configured in the 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 drop-down list, select **None**.

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

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

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

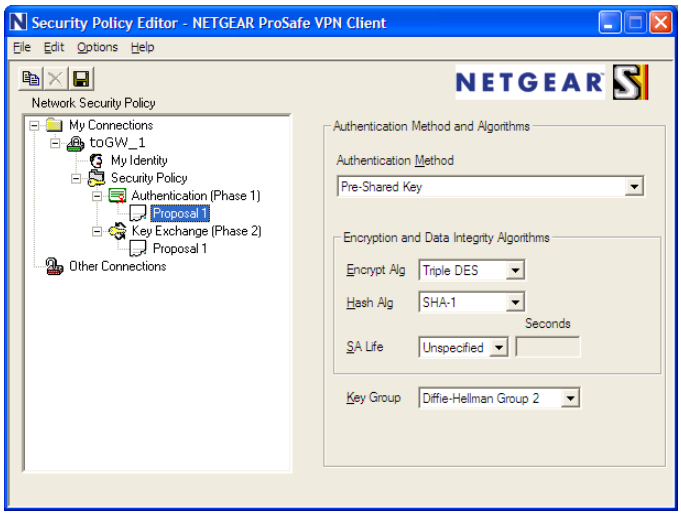

f. Click **Enter Key**. Enter the modem router pre-shared key, and then click **OK**. In this example, 12345678 is entered, though asterisks are displayed in the field. This field is case-sensitive.

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 has to match your selection in the modem 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 click **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 that is configured for the Encryption Protocol in the modem router in *Table 3* on page 96. This example uses Triple DES.

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

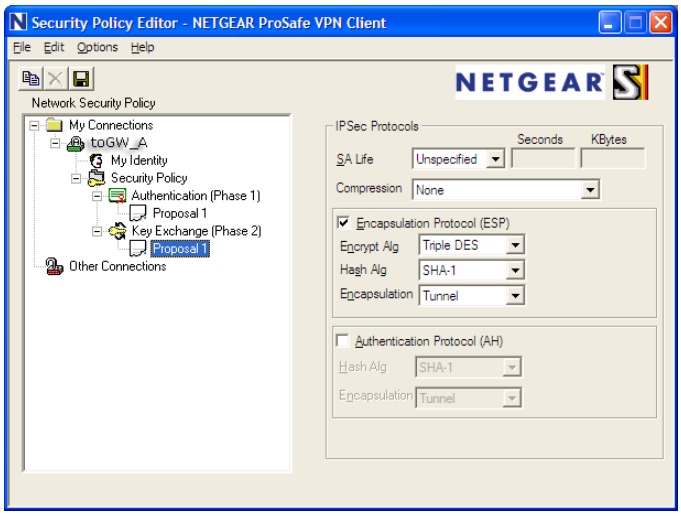
f. In the SA Life drop-down list, select **Unspecified**.

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 has to match your selection in the modem router configuration.

   a. Expand the Key Exchange subheading by double-clicking its name or clicking the + symbol. Then click **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 that is configured for the encryption protocol in the modem router in *Table 3* on page 96. This example uses Triple DES.

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

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

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

7. Save the VPN client settings.

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

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

8. Check the VPN connection.

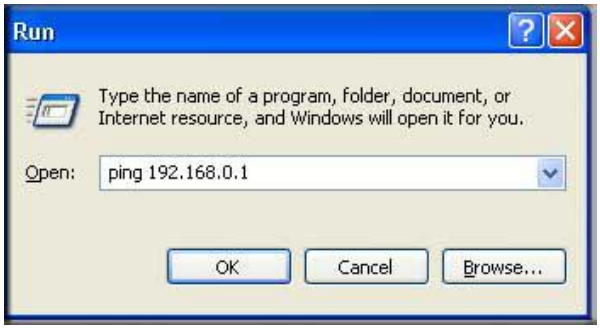
To check the VPN connection, you can initiate a request from the remote PC to the modem router's network by using the Connect option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client reports the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address,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

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

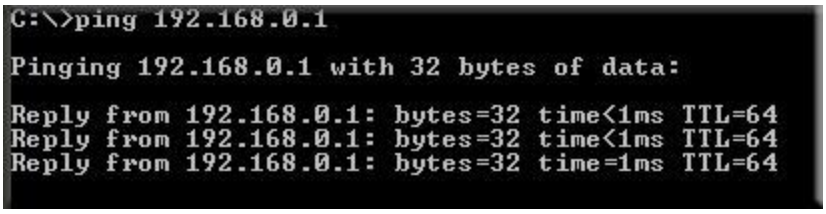
**a.** Establish an Internet connection from the PC.

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

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



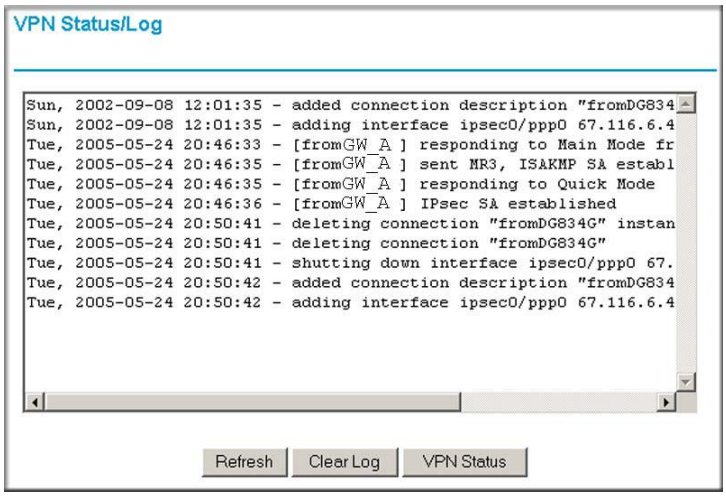

This causes a continuous ping to be sent to the first modem router. After between several seconds and 2 minutes, the ping response should change from timed out to reply.




Once the connection is established, you can open a browser on the PC and enter the LAN IP address of the remote gateway. After a short wait, you should see the login screen of the modem router (unless another PC is already logged in to the modem router).

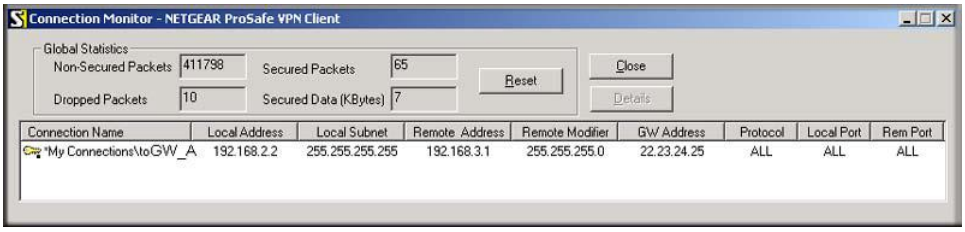
You can view information about the progress and status of the VPN client connection by opening the NETGEAR ProSafe Log Viewer.

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




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

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




In this example you can see these settings:

- The modem router has a GW address (public IP WAN address) of 22.23.24.25.
- The modem router has a remote address (LAN IP address) of 192.168.3.1.
- The VPN client PC has a local address (dynamically assigned address) of 192.168.2.2.

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

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

# Set Up a Gateway-to-Gateway VPN Configuration

This section describes how to use the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in *Table 4* on page 97. If you have special requirements not covered by these VPNC-recommended parameters, see *Set Up VPN Tunnels in Special Circumstances* on page 118 for information about how to set up the VPN tunnel.

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

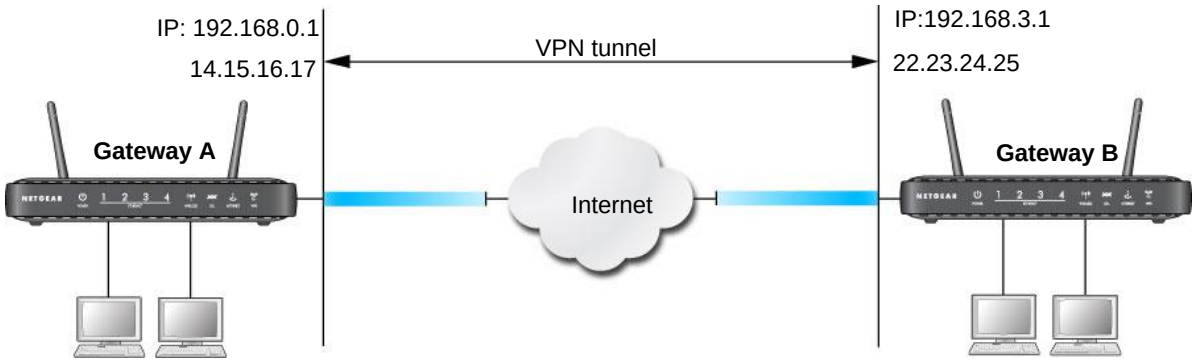



**Figure 21. Gateway-to-gateway VPN tunnel**

Set the LAN IPs on each modem router to a different subnet and configure each correctly for the Internet. The subsequent examples assume the settings shown in the following table.

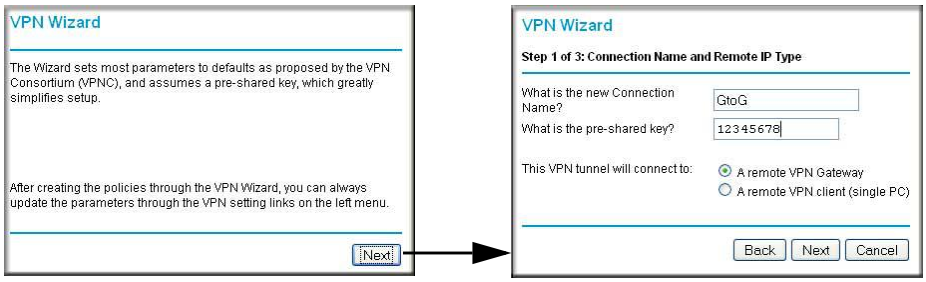
**Table 6. Gateway-to-Gateway VPN Tunnel Configuration Worksheet**

| **Parameter** | | **Value to Be Entered** | **Field Selection** | |
|---|---|---|---|---|
| Connection Name | | GtoGr | N/A | |
| Pre-Shared Key | | 12345678 | N/A | |
| Secure Association | | N/A | Main Mode | Manual Keys |
| Perfect Forward secrecy | | N/A | Enabled | Disabled |
| Encryption Protocol | | N/A | DES | 3DES |
| Authentication Protocol | | N/A | MD5 | SHA-1 |
| Diffie-Hellman (DH) Group | | N/A | Group 1 | Group 2 |
| Key Life in seconds | | 28800 (8 hours) | N/A | |
| IKE Life Time in seconds | | 3600 (1 hour) | N/A | |
| **VPN Endpoint** | **Local IPSecID** | **LAN IP Address** | **Subnet Mask** | **FQDN or Gateway IP (WAN IP Address)** |
| Gateway_A | GW_A | 192.168.0.1 | 255.255.255.0 | 14.15.16.17 |
| Gateway_B | GW_B | 192.168.3.1 | 255.255.255.0 | 22.23.24.25 |

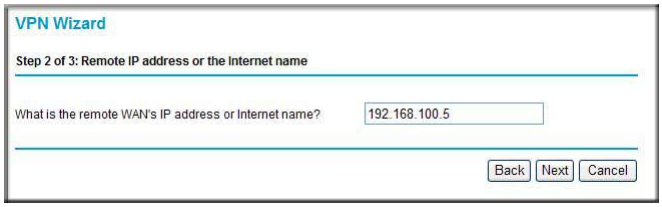
The LAN IP address ranges of each VPN endpoint has to be different. The connection will fail if both are using the NETGEAR default address range of 192.168.0.x.

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

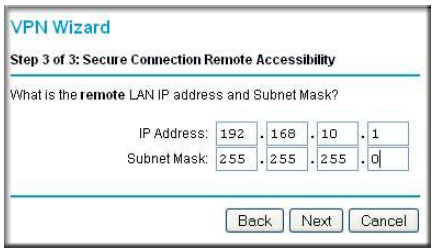
1. Log in to Gateway A on LAN A. Select **VPN Wizard**. Click **Next**, and the Step 1 of 3 screen displays.




2. Fill in the Connection Name field and pre-shared key fields. Select the radio button for the type of target end point, and click **Next**, and the Step 2 of 3 screen displays.




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

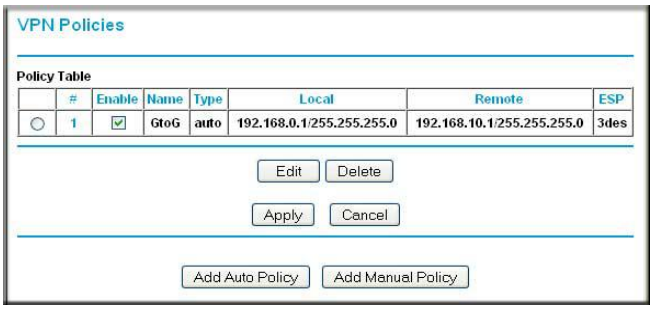



4. Fill in the IP Address and Subnet Mask fields for the target endpoint that can use this tunnel, and click **Next**.

The VPN Wizard Summary screen displays:


To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the **here** link.

5. Click **Done** on the Summary screen.
6. The VPN Policies screen displays, showing that the new tunnel is enabled.

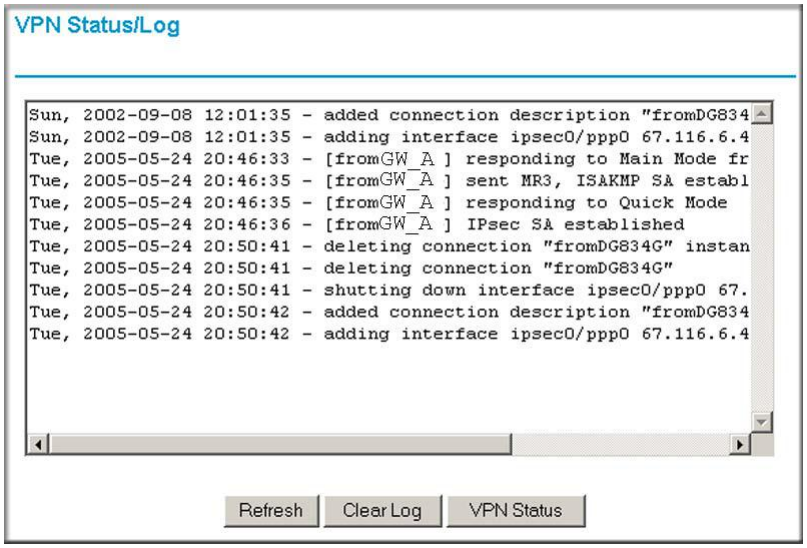



**Note:** See *Use Auto Policy to Configure VPN Tunnels* on page 118 for information about how to enable the IKE keepalive capability on an existing VPN tunnel.

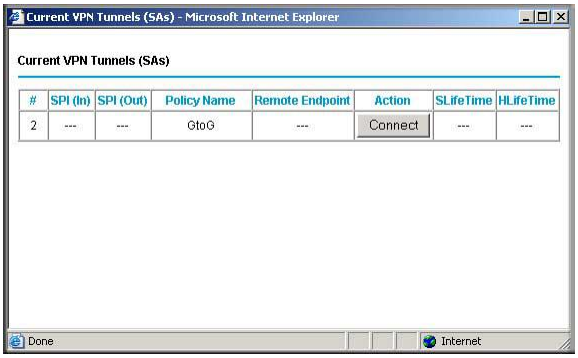
7. Repeat these steps for the gateway on LAN B, and pay special attention to the following network settings:
   - WAN IP of the remote VPN gateway (for example, **14.15.16.17**)
   - LAN IP settings of the remote VPN gateway:
     - IP address (for example, **192.168.0.1**)
     - Subnet mask (for example, **255.255.255.0**)
     - Preshared key (for example, **12345678**)
8. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

**Note:** The VPN Status screen is only one of three ways to active a VPN tunnel. See *Activate a VPN Tunnel* on page 112 for information about the other ways.

**a.** On the modem router menu, select **VPN Status**. The VPN Status/Log screen displays:




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




**c.** Click **Connect** for the VPN tunnel you want to activate. View the VPN Status/Log screen to verify that the tunnel is connected.

# VPN Tunnel Control

## Activate a VPN Tunnel

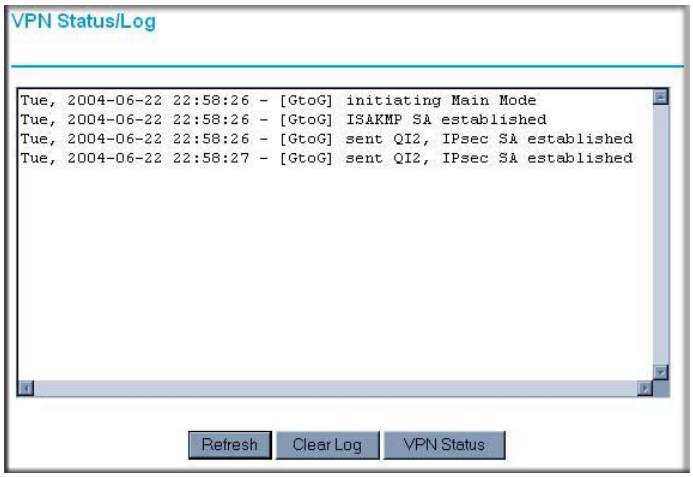
There are three ways to activate a VPN tunnel:

- Use the VPN Status screen.
- Ping the remote endpoint.
- Start using the VPN tunnel.

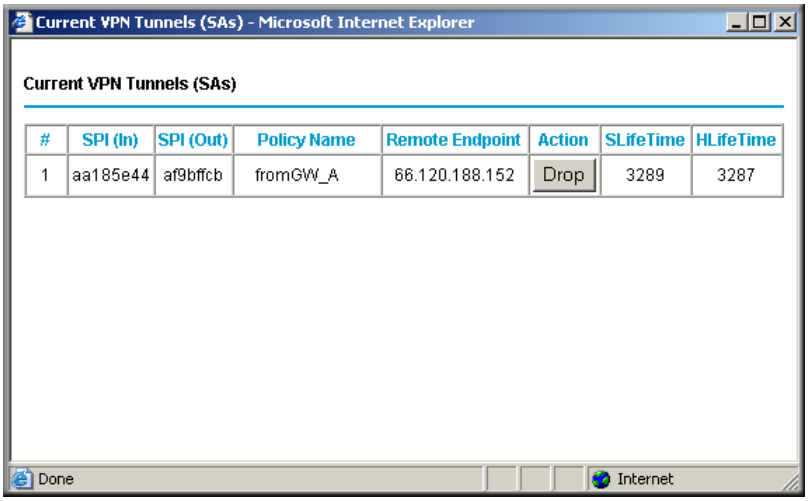
**Note:** See *Use Auto Policy to Configure VPN Tunnels* on page 118 for information about how to enable the IKE keep-alive capability on an existing VPN tunnel.

### *Use the VPN Status Screen to Activate a VPN Tunnel*

1. Select **Advanced - VPN > VPN Status**. The VPN Status/Log screen displays:



2. Click **VPN Status** to display the Current VPN Tunnels (SAs) screen:




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

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

> **Note:** This section uses 192.168.3.1 for sample remote endpoint LAN IP address.

To activate the VPN tunnel by pinging the remote endpoint (for example, 192.168.3.1), perform the following steps depending on whether your configuration is client-to-gateway or gateway-to-gateway:

- **Client-to-gateway configuration**. To check the VPN connection, you can initiate a request from the remote PC to the DGN2200's network by using the Connect option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client reports the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it has to initiate the request.

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

  **a.** Establish an Internet connection from the PC.

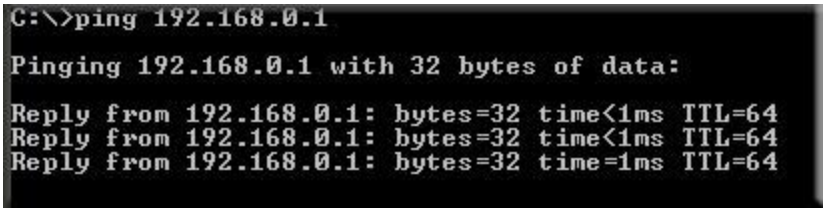
  **b.** On the Windows taskbar, click the **Start** button, and then select **Run**.

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


Running a ping test to the LAN from the PC

This causes a continuous ping to be sent to the first DGN2200. Within 2 minutes, the ping response should change from timed out to reply.

**Note:** You can use Ctrl-C to stop the pinging.

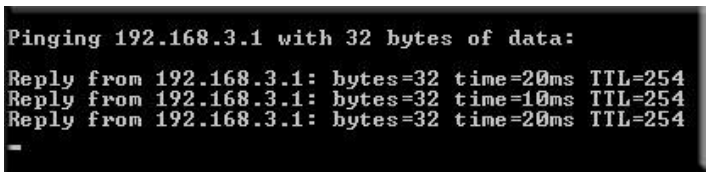



Once the connection is established, you can open a browser on the PC and enter the LAN IP address of the remote DGN2200. After a short wait, you should see the login screen of the modem router (unless another PC already has the DGN2200 management interface open).

- **Gateway-to-gateway configuration**. Test the VPN tunnel by pinging the remote network from a PC attached to Gateway A (the modem router).

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

  **b.** Type **ping 192.168.3.1**.



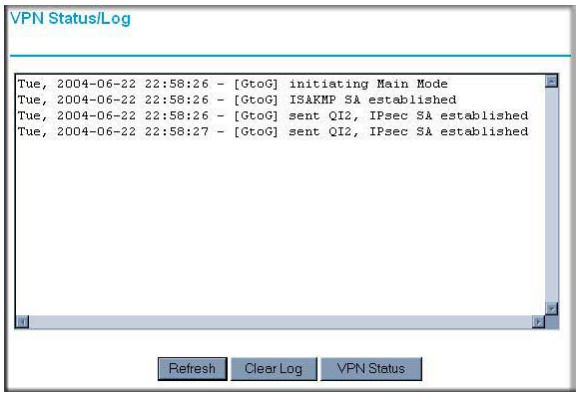

**Note:** The pings might fail the first time. If they do, then try the pings a second time.

### *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.

# Verify the Status of a VPN Tunnel

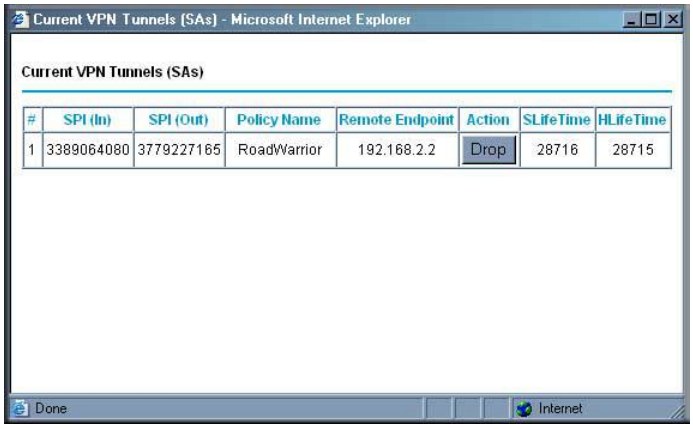
1. Select **Advanced - VPN > VPN Status** to display the VPN Status/Log screen.




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.

2. Click **VPN Status** to display the Current VPN Tunnels (SAs) screen.




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

- **SPI**. Each SA has a unique SPI (Security Parameter Index) for traffic in each direction. For manual key exchange, the SPI is specified in the policy definition. For automatic key exchange, the SPI is generated by the IKE protocol.
- **Policy Name**. The VPN policy associated with this SA.
- **Remote Endpoint**. The IP address on the remote VPN endpoint.
- **Action**. Either a Drop or a Connect button.
- **SLifeTime (Secs)**. The remaining soft lifetime for this SA in seconds. When the soft lifetime becomes 0 (zero), the SA (security association) is re-negotiated.

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

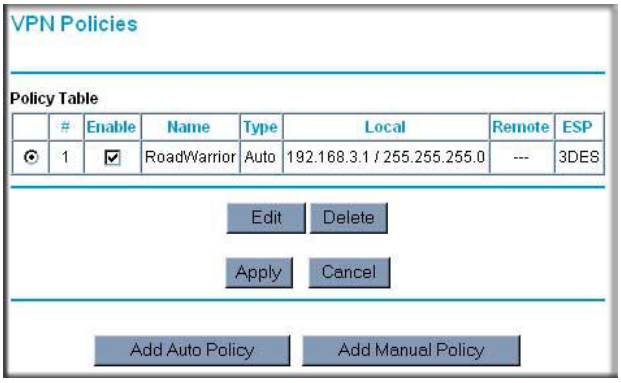
## Deactivate a VPN Tunnel

Sometimes a VPN tunnel has to be deactivated for testing purposes. You can deactivate a VPN tunnel from two places:

- Policy table on VPN Policies screen
- VPN Status screen

### *Use the Policy Table on the VPN Policies Screen to Deactivate a VPN Tunnel*

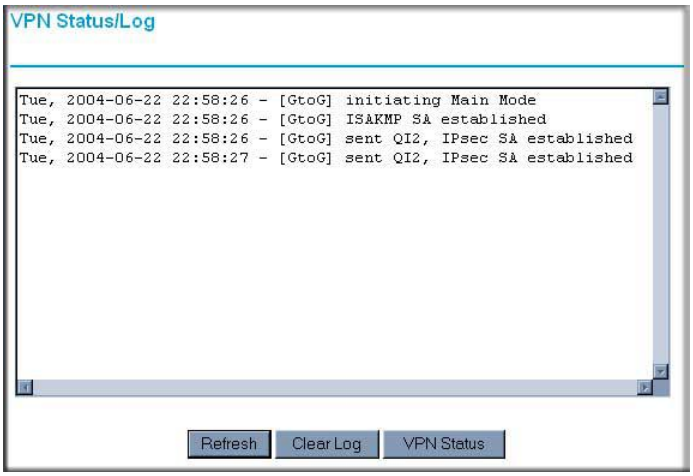
1. Select **Advanced - VPN > VPN Policies** to display the VPN Policies screen.



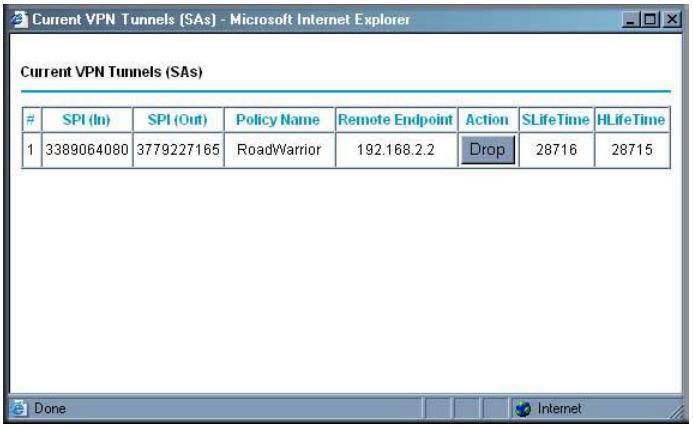

2. In the Policy Table, clear the **Enable** check box for the VPN tunnel that you want to deactivate, and then click **Apply**. (To reactivate the tunnel, select the **Enable** check box, and then click **Apply**.)

## *Use the VPN Status Screen to Deactivate a VPN Tunnel*

1. Select **Advanced - VPN > VPN Status** to display the VPN Status screen.



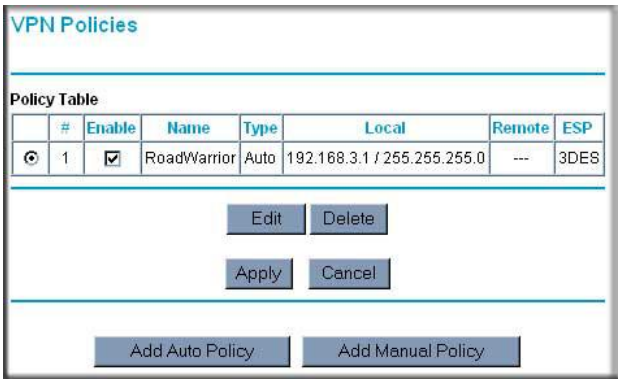

2. Click **VPN Status**. The Current VPN Tunnels (SAs) screen displays:




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

## Delete a VPN Tunnel

1. Select **Advanced - VPN > VPN Policies** to display the VPN Policies screen.




2. In the Policy Table, select the radio button for the VPN tunnel to be deleted, and then click **Delete**.

# Set Up VPN Tunnels in Special Circumstances

When the VPN Wizard and its VPNC defaults (see *Table 4* on page 97) are not appropriate for your circumstances, use one of these alternatives:

- **Auto Policy**. For a typical automated Internet Key Exchange (IKE) setup, see *Use Auto Policy to Configure VPN Tunnels* on page 118. 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 have to specify each phase of the connection, see *Use Manual Policy to Configure VPN Tunnels* on page 125. 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 DGN2200 and the corresponding VPN endpoint gateway or client workstation.

## Use Auto Policy to Configure VPN Tunnels

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

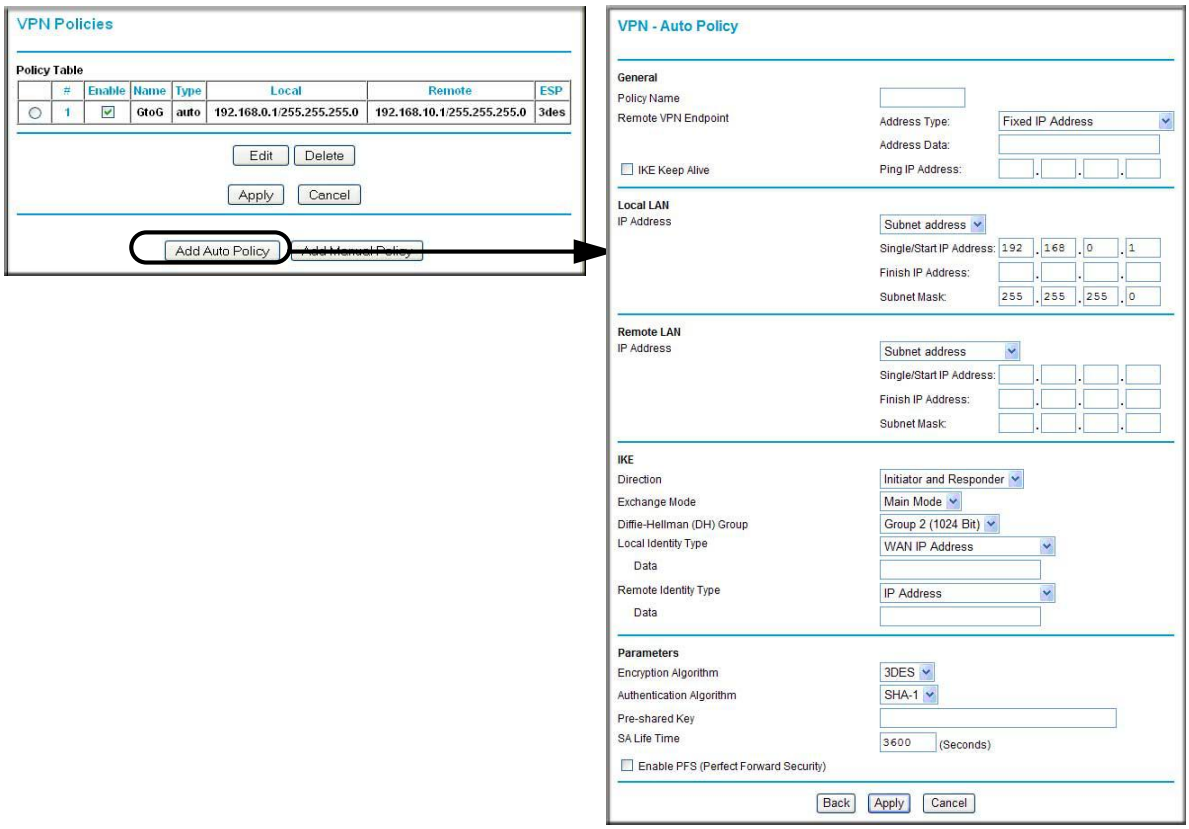
See *Example of Using Auto Policy* on page 122 for an example of using Auto Policy.

### *Configure VPN Network Connection Parameters*

All VPN tunnels on the modem router require that you configure several network parameters. This section describes those parameters and how to access them.

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

Select **Advanced - VPN > VPN Policies**, and click the **Add Auto Policy** button to display the VPN - Auto Policy screen:




The DGN2200 VPN tunnel network connection fields are defined in the following sections.

## *VPN Auto Policy General Settings*

- **Policy Name**. Enter a unique name. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**. The remote VPN endpoint has to have this VPN gateway's address entered as its remote VPN endpoint.

  If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (**IP address** or **domain name**) and enter the address of the remote VPN endpoint to which you want to connect.
- **IKE Keep Alive**. If you want to ensure that a connection is kept open, or, if that is not possible, that it is quickly re-established when a connection is lost select this check box.

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

### *VPN Auto Policy Local LAN Settings*

The remote VPN endpoint needs to have these IP addresses entered as its remote addresses.

- **Subnet Mask**. The network mask.
- **Single/Start IP Address**s. Enter the IP address for a single address, or the starting address for an address range. A single address setting is used when you want to make a single server on your LAN available to remote users. A range has to be an address range used on your LAN. **Any**. The remote VPN endpoint might be at any IP address.
- **Finish IP Address**. For an address range, enter the finish IP address. This needs to be an address range used on your LAN.

### *VPN Auto Policy Remote LAN Settings*

The remote VPN endpoint has to have these IP addresses entered as its local addresses.

- **IP Address**. If there is no LAN (only a single PC) at the remote endpoint, select **Single PC - no Subnet** option. If this option is selected, no additional data is required. The typical application is a PC running the VPN client at the remote end.
- **Single/Start IP Address**. Enter an IP address that is on the remote LAN. You can use this setting when you want to access a server on the remote LAN.
  - For a range of addresses, enter the starting IP address. This needs to be an address range used on the remote LAN.
  - **Any**. Any outgoing traffic from the computers in the **Local IP** fields triggers an attempted VPN connection to the remote VPN endpoint. Be sure you want this option before selecting it.
- Finish IP Address. Enter the finish IP address for a range of addresses. This has to be an address range used on the remote LAN.
- Subnet Mask. Enter the network mask.

### *VPN Auto Policy IKE Settings*

- **Direction**. This setting is used when the modem router determines if the IKE policy matches the current traffic. Select an option.
  - **Responder only**. Incoming connections are allowed, but outgoing connections are blocked.
  - **Initiator and Responder**. Both incoming and outgoing connections are allowed.
- **Exchange Mode**. Ensure that the remote VPN endpoint is set to use Main Mode.

- **Diffie-Hellman (DH) Group**. The Diffie-Hellman algorithm is used when keys are exchanged. The DH Group setting determines the bit size used in the exchange. This value needs to match the value used on the remote VPN gateway.
- **Local Identity Type**. Select an option to match the Remote Identity Ty**pe** setting on the remote VPN endpoint.
  - **WAN IP Address**. Your Internet IP address.
  - **Fully Qualified Domain Name**. Your domain name.
- **Fully Qualified User Name**. Your name, e-mail address, or other ID.
- **Local Identity Data**. Enter the data for the local identity type that you selected. (If WAN IP Address is selected, no input is required.)
- **Remote Identity Type**. Select the option that matches the Local Identity Type setting on the remote VPN endpoint.
  - **IP Address**. The Internet IP address of the remote VPN endpoint.
  - **Fully Qualified Domain Nam**e. The domain name of the remote VPN endpoint.
  - **Fully Qualified User Name**. The name, email address, or other ID of the remote VPN endpoint.
- **Remote Identity Data**. Enter the data for the remote identity type that you selected. If IP Address is selected, no input is required.

### *VPN Auto Policy Parameters*

- **Encryption Algorithm**. The encryption algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. DES and 3DES are supported.
  - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.
  - **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- **Authentication Algorithm**. The authentication algorithm used for both IKE and IPSec. This setting has to 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**. 160 bits, slower but more secure. This is the default.
- **Pre-shared Key**. The key has to be entered both here and on the remote VPN gateway.
- **SA Life Time**. The time interval before the SA (security association) expires. (It is automatically reestablished as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA life time. This setting applies to both IKE and IPSec SAs.
- **Enable IPSec PFS (Perfect Forward Secrecy)**. If this check box is selected, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

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

## *Example of Using Auto Policy*

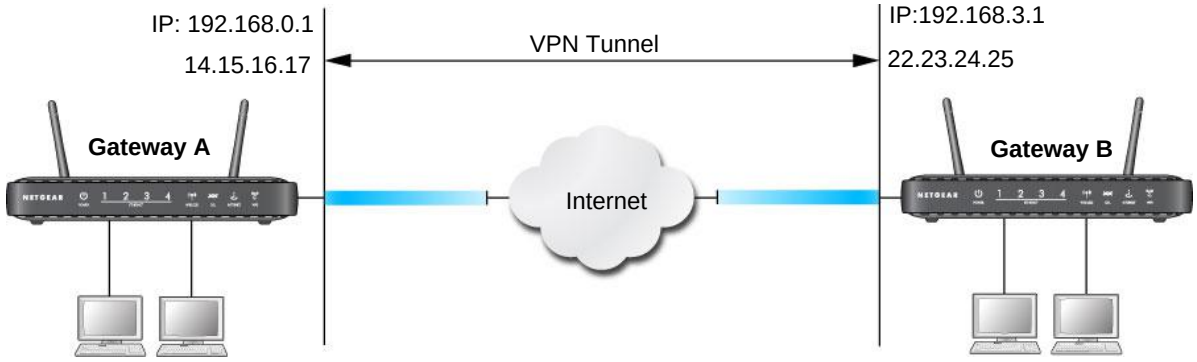



**Figure 22. Auto Policy**

The following settings are assumed for this example:.

**Table 7. Gateway-to-Gateway VPN Tunnel Configuration Worksheet**

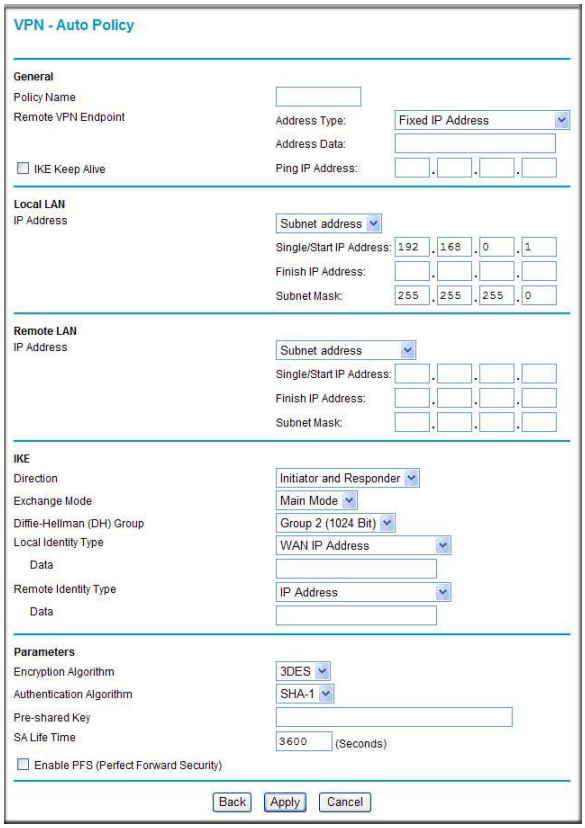
| **Parameter** | | **Value to Be Entered** | **Field Selection** | |
|---|---|---|---|---|
| Connection Name | | GtoG | N/A | |
| Pre-Shared Key | | 12345678 | N/A | |
| Secure Association | | N/A | Main Mode | Manual Keys |
| Perfect Forward secrecy | | N/A | Enabled | Disabled |
| Encryption Protocol | | N/A | DES | 3DES |
| Authentication Protocol | | N/A | MD5 | SHA-1 |
| Diffie-Hellman (DH) Group | | N/A | Group 1 | Group 2 |
| Key Life in seconds | | 28800 (8 hours) | N/A | |
| IKE Life Time in seconds | | 3600 (1 hour) | N/A | |
| **VPN Endpoint** | **Local IPSecID** | **LAN IP Address** | **Subnet Mask** | **FQDN or Gateway IP (WAN IP Address** |
| Gateway_A | GW_A | 192.168.0.1 | 255.255.255.0 | 14.15.16.17 |
| Gateway_B | GW_B | 192.168.3.1 | 255.255.255.0 | 22.23.24.25 |

### To use Auto Policy:

1. Set the LAN IPs on each modem router to different subnets and configure each correctly for the Internet.

2. Select **Advanced - VPN > VPN Policies** and click the **Add Auto Policy** button.

   The VPN Auto Policy screen displays:

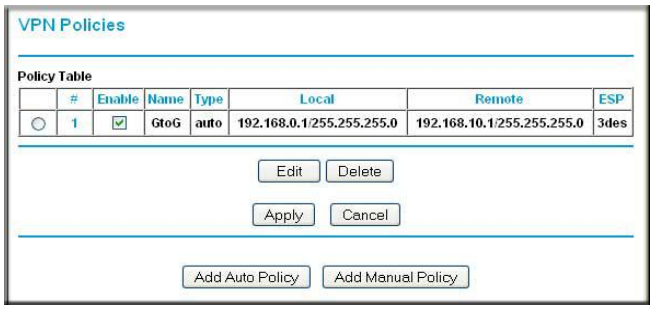



3. Enter these policy settings:

| Auto Policy Field | | Description |
|---|---|---|
| General | Policy Name | GtoG |
| | Remote VPN Endpoint Address Type | Fixed |
| | Remote VPN Endpoint Address Data | 22.23.24.25 |
| Local LAN | | Use the default settings. |
| Remote LAN | IP Address | Select **Subnet address** from the drop-down list. |
| | Start IP Address | 192.168.3.1 |
| | Subnet Mask | 255.255.255.0 |

| Auto Policy Field | | Description |
|---|---|---|
| IKE | Direction | Initiator and Responder |
| | Exchange Mode | Main Mode |
| | Diffie-Hellman (DH) Group | Group 2 (1024 Bit) |
| | Local Identity Type | Use the default setting. |
| | Remote Identity Type | Use the default setting. |
| Parameters | Encryption Algorithm | 3DES |
| | Authentication Algorithm | MD5 |
| | Pre-shared Key | 12345678 |

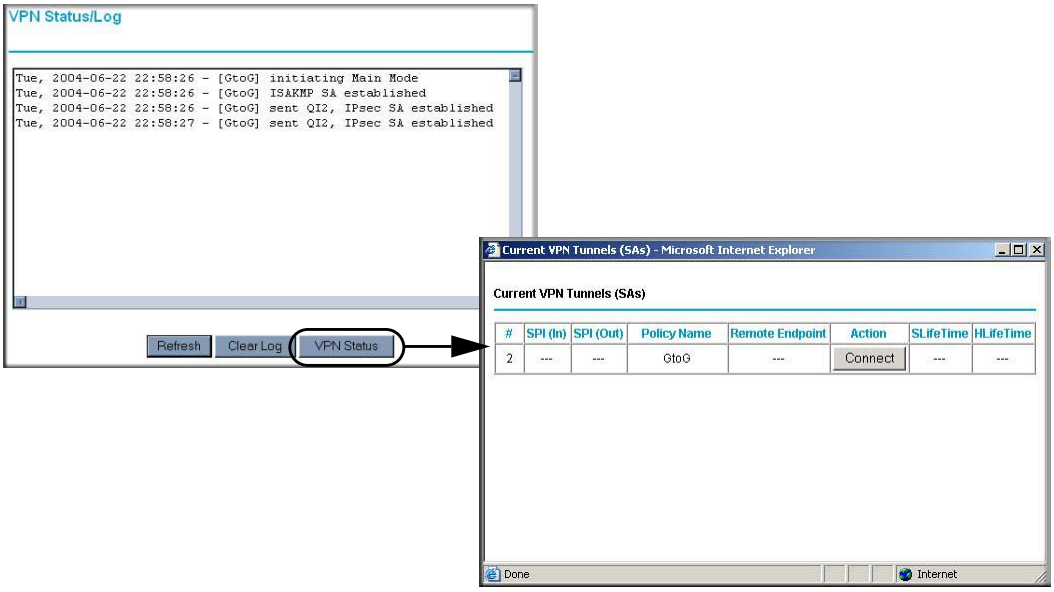
4. Click **Apply**. The VPN Policies screen displays:




5. Repeat these steps for the DGN2200 on LAN B. Pay special attention to the following network settings:
   - General, Remote Address Data (for example, 14.15.16.17)
   - Remote LAN, Start IP Address
     - IP Address (for example, 192.168.0.1)
     - Subnet Mask (for example, 255.255.255.0)
     - Pre-shared Key (for example, 12345678)
6. Use the VPN Status screen to activate the VPN tunnel:

**Note:** The VPN Status screen is only one of three ways to active a VPN tunnel. See *Activate a VPN Tunnel* on page 112 for information about the other ways.

**a.** Select **VPN > VPN Status** to display the VPN Status/Log screen. Then click **VPN Status** to display the Current VPN Tunnels (SAs) screen:

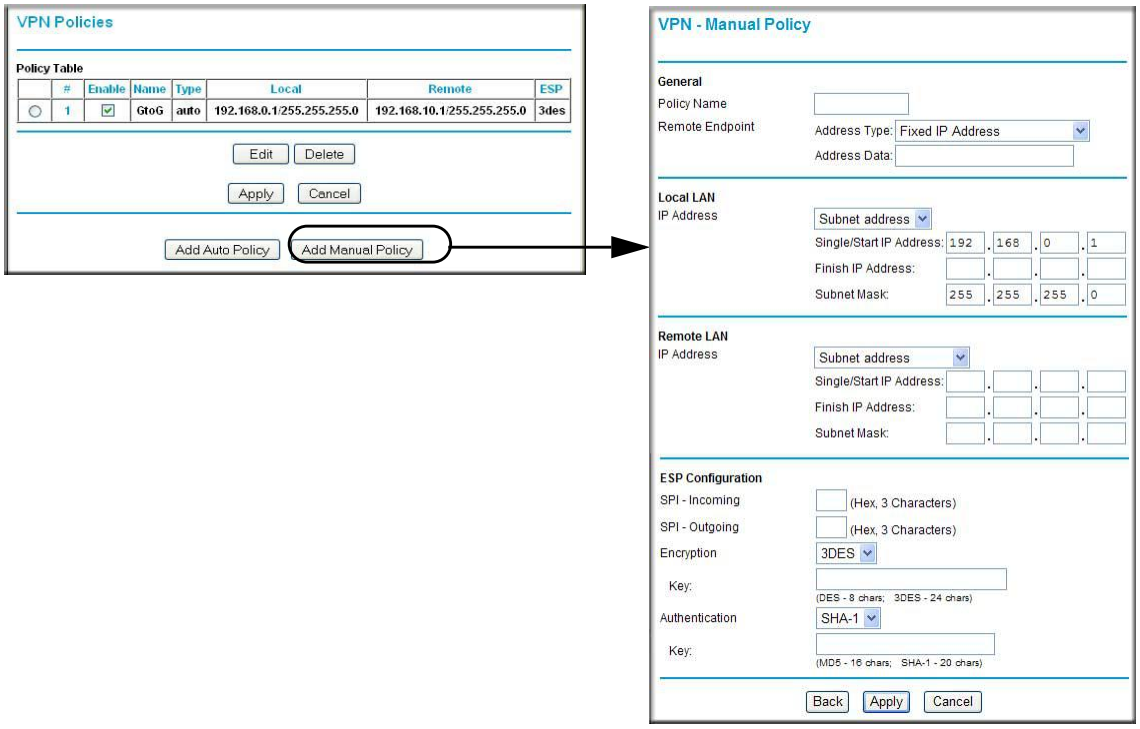



**b.** Click **Connect** for the VPN tunnel that you want to activate. Review the VPN Status/Log screen (*Figure a* on page 111) to verify that the tunnel is connected.

## Use Manual Policy to Configure VPN Tunnels

As an alternative to IKE, you can use manual keying, in which you need to 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).

Select **Advanced - VPN > VPN Policies**, and then click the **Add Manual Policy** radio button to display the VPN - Manual Policy screen:




The following sections explain the fields in the VPN Manual Policy screen.

## *VPN Manual Policy General Settings*

The DGN2200 VPN tunnel network connection fields are 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**. The remote VPN endpoint has to have this VPN gateway's address entered as its remote VPN endpoint.

  If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (IP address or domain name) and enter the address of the remote VPN endpoint to which you want to connect.

## *VPN Manual Policy Local LAN Settings*

The remote VPN endpoint has to have these IP addresses entered as its remote addresses.

- **Subnet Address**. Enter the network mask.
- **Single PC - no Subnet**. Select this option if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required.

- **Single/Start IP Address**. The IP address for a single address, or the starting address for an address range used on the LAN. If you want to make a single server on your LAN available to remote users, use a single address Any settings. The remote VPN endpoint can be at any IP address.
- **Finish IP Address**. For an address range, enter the finish IP address. This has to be an address range used on your LAN.
- **Subnet Mask**. Enter the network mask.

### *VPN Manual Policy Remote LAN Settings*

The remote VPN endpoint has to have these IP addresses entered as its local addresses.

- **IP Address**. Select **Single PC - no Subnet** if there is no LAN (only a single PC) at the remote endpoint. If this option is selected, no additional data is required. The typical application is a PC running the VPN client at the remote end.
- **Single/Start IP Address**. Enter an IP address on the remote LAN. You can use this setting to access a server.
  - For a range of addresses, enter the starting IP address. This has to be an address range used on the remote LAN.
  - **Any**. Any outgoing traffic from specified Local IP computers triggers an attempted VPN connection to the remote VPN endpoint. Be sure you want this option before selecting it.
- **Finish IP Address**. Enter the finish IP address for a range of addresses. This has to be an address range used on the remote LAN.
- **Subnet Mask**. Enter the network mask.

### *VPN Manual Policy ESP Settings*

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 has to have unique SPIs. These settings need to match the remote VPN endpoint. The **in** setting here has to match the **out** setting on the remote VPN endpoint, and the **out** setting here has to match the **in** setting on the remote VPN endpoint.
- **Encryption**. Select an encryption algorithm, and enter the key in the field provided. For 3DES, the keys should be 24 ASCII characters, and for DES, the keys should be 8 ASCII characters.
  - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.
  - **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- **Authentication**. Specify the authentication and the key.

# Troubleshooting

# 9

## Diagnosing and Solving Problems

This chapter provides information to help you diagnose and solve problems you might have with your 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:

# Troubleshooting with the LEDs

When you turn the power on, the power, LAN, and DSL 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, the LAN and DSL LEDs light as follows:
   a. The LAN port LEDs light for any local ports that are connected.
   b. The DSL link LED lights to indicate that there is a link to the connected device.
   c. If a LAN port is connected to a 100 Mbps device, verify that the LAN port's LED is green. Note that if the LAN port is 10 Mbps, the LED is amber.

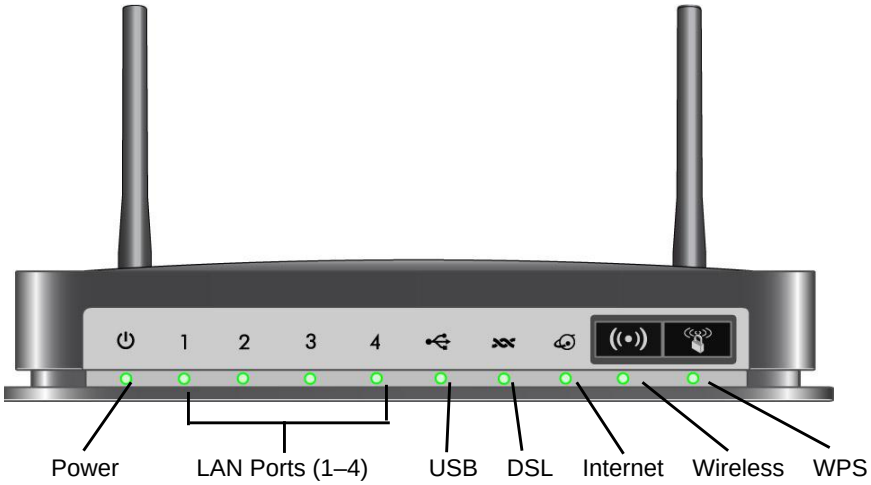



**Figure 23. Front panel LEDs**

## Power LED Is Off

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

- Check that the power cord is correctly connected to your modem 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 modem 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 modem router.

If the Power LED turns red to indicate a modem router fault, turn the power off and on to see if the 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 modem router recovers.
- Clear the modem router's configuration to factory defaults as explained in *Factory Settings* on page 138. This sets the modem 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 appropriate LAN LED does not light when the Ethernet connection is made, check the following:

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

## Cannot Log In to the Wireless-N Modem Router

If you are unable to log in to the modem router 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 modem router as described in the previous section.
- Make sure that your computer's IP address is on the same subnet as the modem router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. Follow the instructions in the online document that you can access from *Preparing Your Network* in Appendix D for information about how to configure your computer.
- 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 modem router, and reboot your computer.
- If your modem router's IP address was changed and you do not know the current IP address, clear the modem router's configuration to factory defaults. This sets the modem router's IP address to 192.168.0.1. This procedure is explained in *Factory Settings* in Appendix A.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.

- Make sure you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

# Troubleshooting the Internet Connection

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

## ADSL Link

If your modem 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.

### *ADSL Link LED Is Green*

If your ADSL link LED is 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.

### *ADSL Link LED Is Blinking Green*

If your ADSL link LED is blinking green, 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 ADSL link LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure 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 ADSL link LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID), then you might have poor-quality wiring in your house.

### *ADSL Link LED Is Off*

If the ADSL link LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure 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 ADSL link 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 might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

## Internet LED Is Red

If the Internet LED is red, the device was unable to connect to the Internet. Verify the following:

- Check that your login credentials are correct, or that the information you entered on the Basic Settings screen is correct.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the ADSL settings screen are correct.
- Check if your ISP has a problem—it might not be that the modem router cannot connect to the Internet but , rahter that your ISP that cannot provide an Internet connection.

## Obtaining an Internet IP Address

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

### To check the Internet IP address from the browser interface:

1. Launch your browser, and select an external site such as *www.netgear.com*.
2. Access the main menu of the modem router's configuration at http://192.168.0.1.
3. In the main menu, under Maintenance, select **Router Status** and 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 modem router is unable to 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 incorrectly set. See the following section, *Troubleshooting PPPoE or PPPoA* .
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP allows only one Ethernet MAC address to connect to 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 modem router's MAC address.
  - Configure your modem router to spoof your computer's MAC address. This can be done in the Basic Settings screen.

## Troubleshooting PPPoE or PPPoA

The PPPoE or PPPoA connection can be debugged as follows:

1. Access the main menu of the modem router at http://192.168.0.1.
2. Select **Maintenance > Router Status**.
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 might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.

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

## Troubleshooting Internet Browsing

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

- Your computer might not recognize any DNS server addresses.

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

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

  If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address as described in the online document that you can access from *Preparing Your Network* in Appendix D.

# 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 Modem Router

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

### To ping the modem 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 modem 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 130.
     - 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 modem 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 modem 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 Modem Router* on page 134 display. If you do not receive replies:

- Check that your PC has the IP address of your modem router listed as the default 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 modem router is listed as the default 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 DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing 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 modem router to clone or spoof the MAC address from the authorized PC.

# Cannot Log in

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

- The modem 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 modem 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 modem router. The LAN LED for the port you are using on the modem router should light up to show your connection.
- Your computer's IP address is on the same subnet as the modem 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 modem router and reboot your computer.
- If your modem router's IP address was changed and you do not know the current IP address, clear the modem router's configuration to factory defaults as explained in *Factory Settings* on page 138. This sets the modem 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 modem router does not save the changes you make in the modem 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.

# Incorrect Date or Time

Select **Security > Schedule** to display the current date and time. The 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 modem router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have just finished setting up the modem router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour. The modem 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 N300 Wireless ADSL2+ Modem Router DGN2200, and instructions for wall-mounting the unit.

This appendix contains the following sections:

# Factory Settings

You can return the modem router to its factory settings. On the bottom of the 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 modem router resets, and returns to the factory settings. Your device will return to the factory configuration settings shown in the following table.

**Table 8. Factory Default Settings**

| Feature | | Default Behavior |
|---|---|---|
| Router Login | User login URL | http://www.routerlogin.com or http://www.routerlogin.net |
| | User name (case-sensitive) | admin |
| | Login password (case-sensitive) | password |
| Internet connection | WAN MAC address | Use default address |
| | WAN MTU size | 1492 |
| | Port speed | Autosensing |
| Local network (LAN) | LAN IP | 192.168.0.1 |
| | Subnet mask | 255.255.255.0 |
| | RIP direction | None |
| | RIP version | Disabled |
| | RIP authentication | None |
| | DHCP server | Enabled |
| Local network (LAN) continued | DHCP starting IP address | 192.168.0.2 |
| | DHCP ending IP address | 192.168.0.254 |
| | DMZ | Enabled or disabled |
| | Time zone | GMT for WW except NA and GR, GMT+1 for GR, GMT-8 for NA |
| | Time zone adjusted for daylight savings time | Disabled |
| | SNMP | Disabled |
| Firewall | 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 |

**Table 8. Factory Default Settings (Continued)**

| Feature | | Default Behavior |
|---|---|---|
| Wireless | Wireless communication | Enabled |
| | SSID name | Can be found on the label on the bottom of the unit. |
| | Security | Can be found on the label on the bottom of the unit. |
| | Broadcast SSID | Enabled |
| | 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 |

# Specifications

| Specification | Description |
|---|---|
| Network protocol and standards compatibility | TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM |
| Power adapter | North America: 120V, 60 Hz, input |
| | UK, Australia: 240V, 50 Hz, input |
| | Europe: 230V, 50 Hz, input |
| | All regions (output): 12V @ 1.5A output |
| Physical | Dimensions: 6.80 in. x 5.03 in. x 1.28 in. (173 mm x 128 mm x 33 mm) |
| | Weight: 0.65 lbs. without the stand (0.29 kg) |
| Environmental | Operating temperature: 0° to 40° C (32º to 104º F) |
| | Operating humidity: 10% to 90% relative humidity, noncondensing |
| | Storage temperature: -20° to 70° C (–4º to 158º F) |
| | Storage humidity: 5 to 95% relative humidity, noncondensing |
| Regulatory compliance | FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B |
| Network protocol and standards compatibility | TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM |
| Power adapter | North America: 120V, 60 Hz, input |
| Regulatory compliance | 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<br>WAN: ADSL, Dual RJ-11, pins 2 and 3<br>T1.413, G.DMT, G.Lite<br>ITU Annex A hardware or Annex B hardware<br>ITU G.992.5 (ADSL2+) |

# Wall-Mount Your Modem Router

Your modem router's location can affect wireless connections. For example, the thickness and number of walls the wireless signal passes through might limit its range. For best results, place your modem router:

- Near an AC power outlet, close to computers you plan to connect with Ethernet cables, and near locations where you use wireless computers. For best signal strength, the modem router should be within line of sight of your wireless devices.
- In an elevated location, keeping the number of walls and ceilings between the modem router and your wireless computers to a minimum.
- Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, or the base for a cordless phone.

### To mount the modem router:

1. Drill holes in the wall where you will wall-mount the modem router.

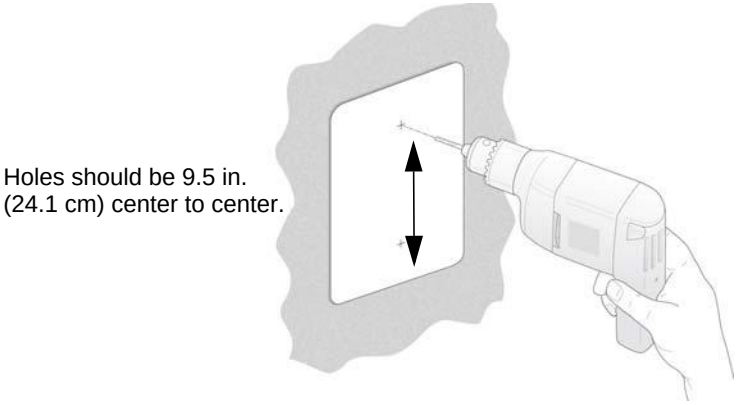



**Figure 24. Drill the holes**

2. Put wall anchors in the holes.

   Use pan head Phillips wood screws, 3.5 x 20 mm (diameter x length, European) or #6 type screw, 1 inch long (U.S.).

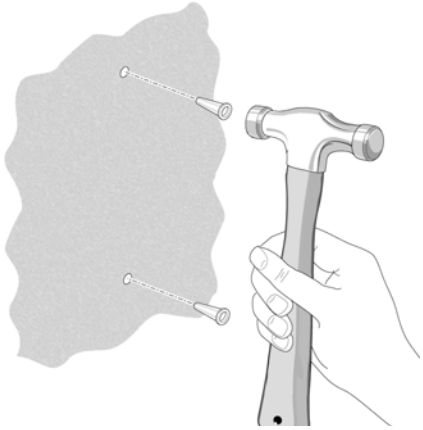


**Figure 25. Put wall anchors in the holes**

3. Insert screws into the wall anchors, leaving 3/16 in. (0.5 cm) of each screw exposed.

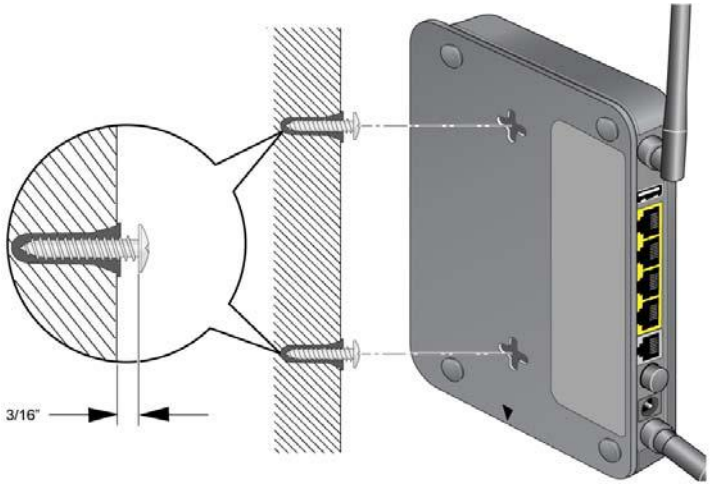



**Figure 26. Insert screws into the wall anchors**

4. For best wireless performance, position the wireless antennas as shown with the top one facing up and the bottom one facing away from the modem router..

**Figure 27. Position the antennas**

# NETGEAR VPN Configuration

# B

This appendix is a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR DGN2200 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 9.**

| 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 preshared secret/key (not certificate based) |
| IP addressing: | | |
| | NETGEAR-Gateway A | Static IP address |
| | NETGEAR-Gateway B | Static IP address |

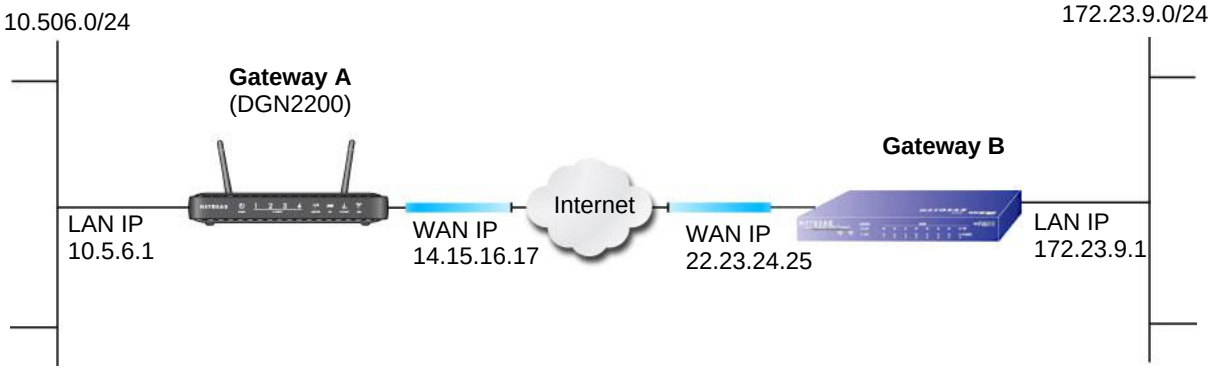



**Figure 28. VPNC Example, Network Interface Addressing**

# Step-by-Step Configuration

1. Use the VPN Wizard to configure Gateway A (DGN2200) for a gateway-to-gateway tunnel (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 108), being certain to use appropriate network addresses for the environment.

   The LAN addresses used in this example are as follows:

**Table 10.**

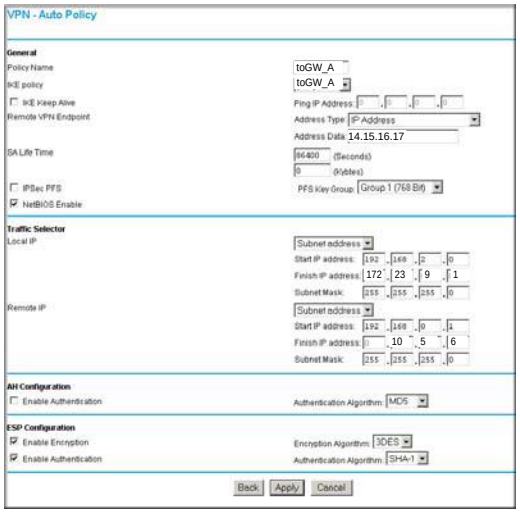
| Unit | WAN IP | LAN IP | LAN Subnet Mask |
|---|---|---|---|
| DGN2200 | 14.15.16.17 | 10.5.6.1 | 255.255.255.0 |
| FVL328 | 22.13.24.25 | 172.23.9.1 | 255.255.255.0 |

   a. Enter **toGW_B** for the connection name.
   b. Enter **22.23.24.25** for the remote WAN's IP address.
   c. Enter the following:
      - IP Address. **172.23.9.1**
      - Subnet Mask. **255.255.255.0**
   d. In the Summary screen, click **Done**.

2. Use the VPN Wizard to configure the Gateway B for a gateway-to-gateway tunnel (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 108), being certain to use appropriate network addresses for the environment.
   a. Enter **toGW_A** for the connection name.
   b. Enter **14.15.16.17** for the remote WAN's IP address.
   c. Enter the following:
      - IP Address. **10.5.6.1**
      - Subnet Mask. **255.255.255.0**
   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:

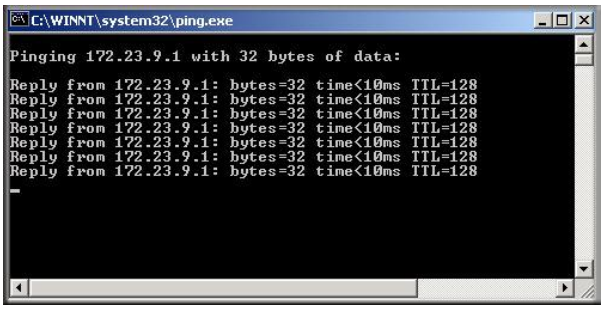



5. Test the VPN tunnel by pinging the remote network from a PC attached to Gateway A (modem router).

   a. Open the command prompt (Start > Run > cmd).

   b. Type **`ping 172.23.9`**.

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



# Modem Router with FQDN to Gateway B

This section is a case study on how to configure a VPN tunnel from a NETGEAR 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.

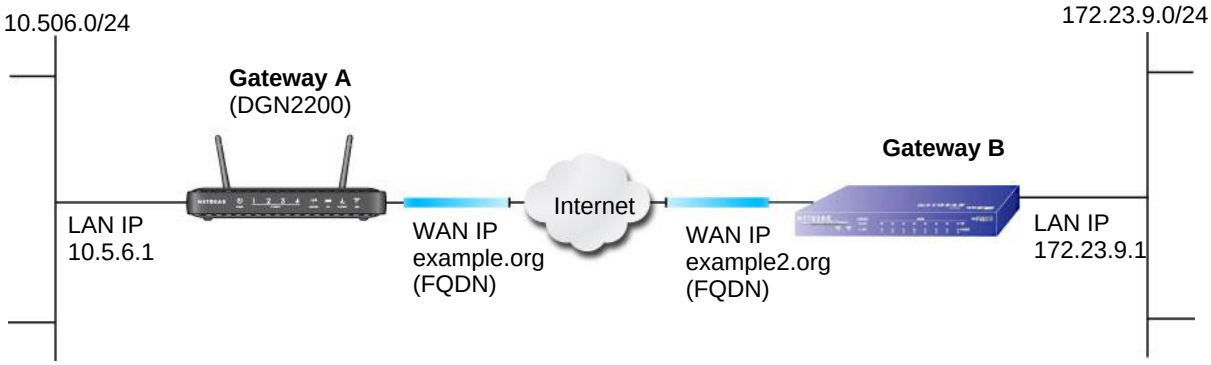



**Figure 29. VPNC Example, Network Interface Addressing**

**Table 11.**

| 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 aualified domain name (FQDN) |
| | NETGEAR-Gateway B | FDQN |

### *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 e-mail addresses, host names, and IP addresses) can be stored and

retrieved. Now, a gateway can be configured to use a third-party service instead of a permanent and unchanging IP address to establish bi-directional VPN connectivity.

To use DDNS, you need to register with a DDNS service provider. Some DDNS service providers include:

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

In this example, Gateway A is configured using a sample FQDN provided by a DDNS service provider. In this case we established the hostname **dg834g.dyndns.org** for Gateway A using the DynDNS service. Gateway B uses the DDNS service provider when establishing a VPN tunnel.

To establish VPN connectivity, Gateway A has to be configured to use Dynamic DNS, and Gateway B has to 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 modem router).

   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.

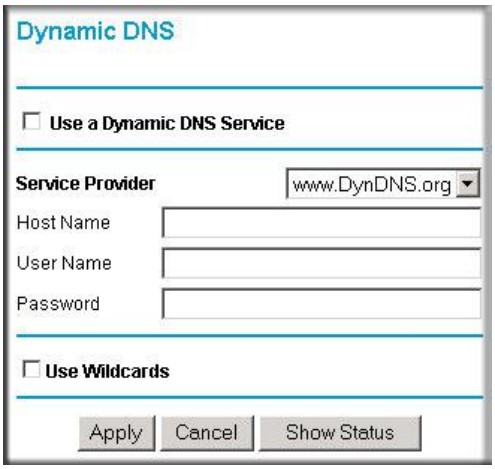
2. On Gateway A, configure the Dynamic DNS settings.

   a. Under the Advanced heading, 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 **gw_a.dyndns.org**.
      - In the **User Name** field, enter the account user name.
      - In the **Password** field, enter the account password.

   c. Click **Apply**.



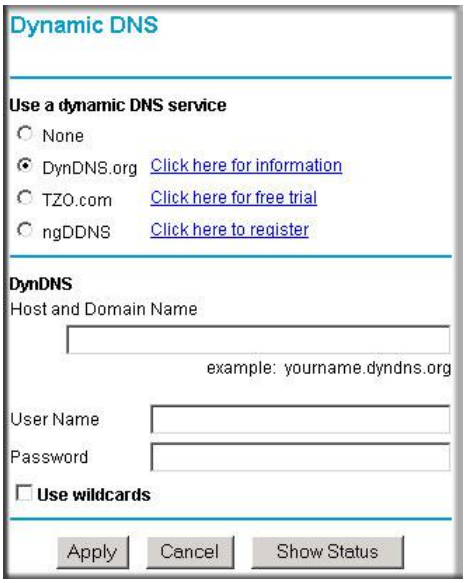
**d.** Click **Show Status**. The resulting screen should show Update OK: good:


**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:



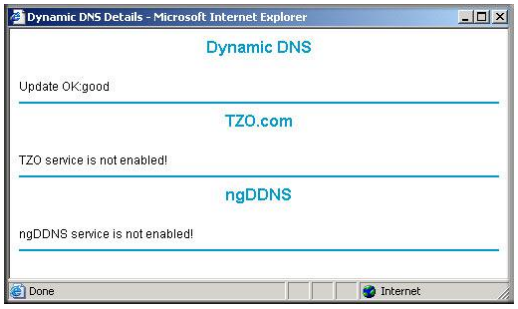

**c.** Fill in the fields with the account and host name settings.

- 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 DGN2200 as in the gateway-to-gateway procedures using the VPN Wizard (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 108), being certain to use appropriate network addresses for the environment.

The LAN addresses used in this example are as follows:

**Table 12.**

| Device | LAN IP Address | LAN Subnet Mask |
|---|---|---|
| DGN2200 | 10.5.6.1 | 255.255.255.0 |
| FVL328 | 172.23.6.1 | 255.255.255.0 |

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

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

**c.** Enter the following:

- IP Address: **172.23.9.1**
- Subnet Mask: **255.255.255.0**

5. Configure the FVL328 as in the gateway-to-gateway procedures for the VPN Wizard (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 108), being certain to use appropriate network addresses for the environment.

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

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

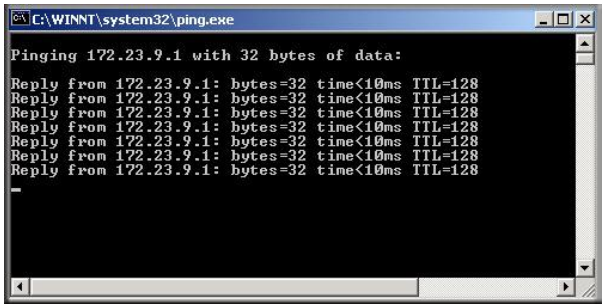
**c.** Enter the following:

- IP Address: **10.5.6.1**
- Subnet Mask: **255.255.255.0**

6. Test the VPN tunnel by pinging the remote network from a PC attached to the DGN2200.

**a.** Open the command prompt (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 13.**

| VPN Consortium Scenario | | Scenario 1 |
|---|---|---|
| Type of VPN: | | PC/client-to-gateway, with client behind NAT router |
| Security scheme: | | IKE with pre-shared secret/key (not certificate based) |
| IP addressing: | | |
| | Gateway | Fully qualified domain name (FQDN) |
| | Client | Dynamic |

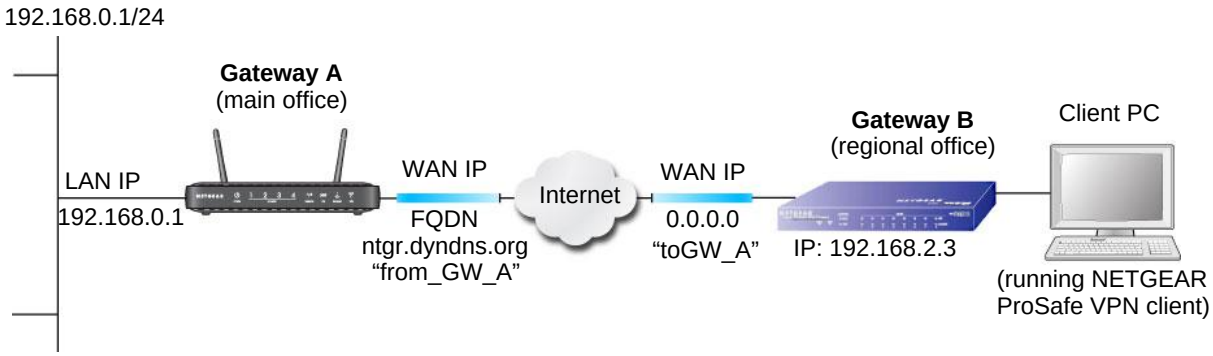



**Figure 30. Telecommuter Example**

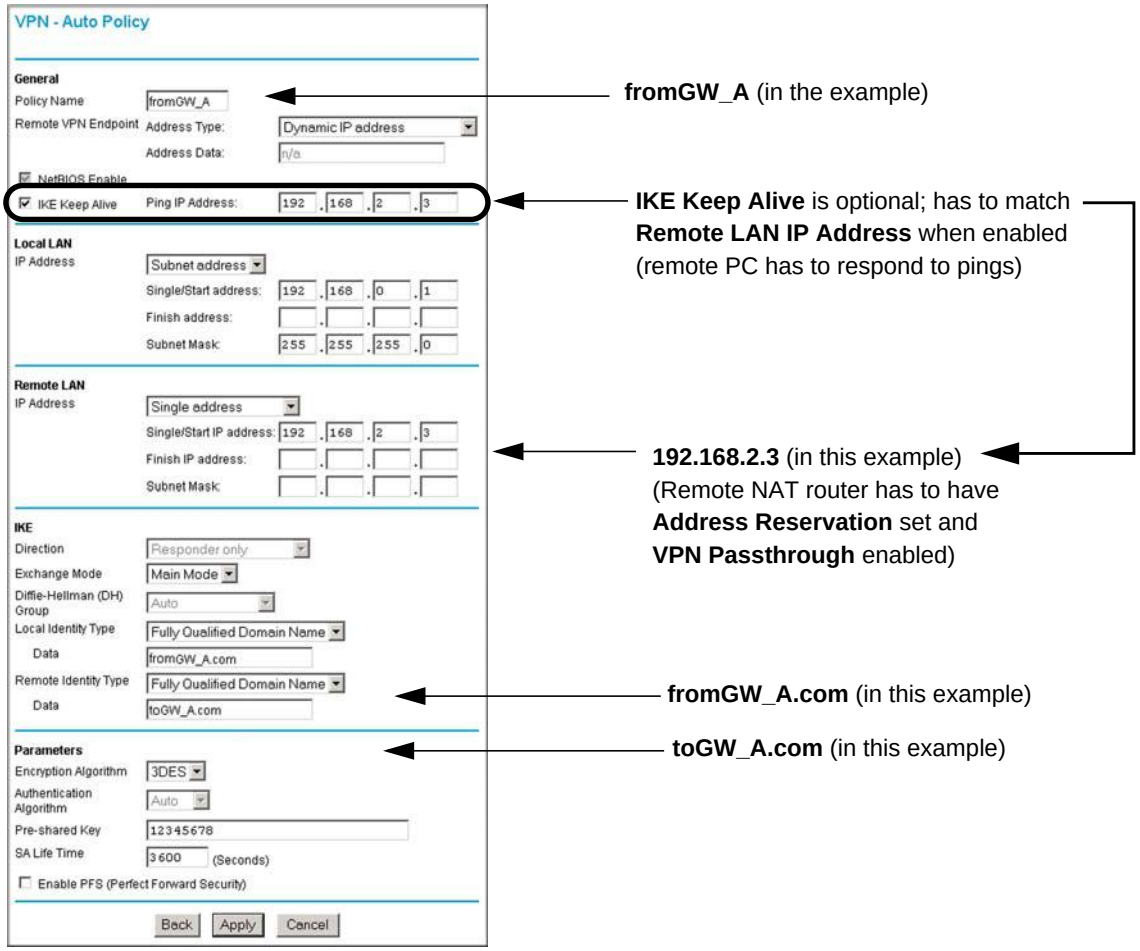
# Setting Up Client-to-Gateway VPN Configuration (Telecommuter Example)

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

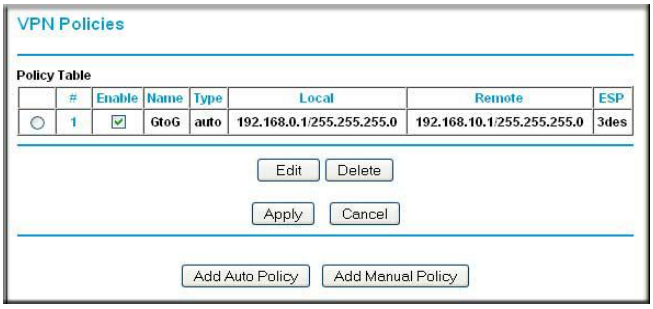
- *Step 1: Configure Gateway A (the NETGEAR VPN Router at the Main Office)* on page 151.
- *Step 2: Configure Gateway B (the Modem Router at the Regional Office)* on page 152 describes configuring the NETGEAR ProSafe VPN Client endpoint.

# Step 1: Configure Gateway A (the NETGEAR VPN Router at the 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.




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




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

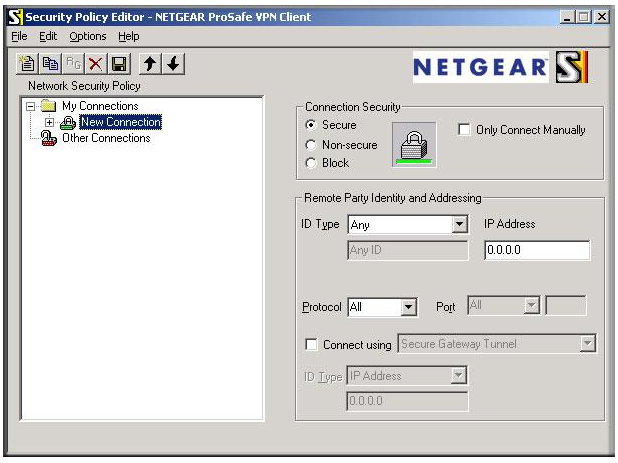
# Step 2: Configure Gateway B (the Modem Router at the Regional Office)

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

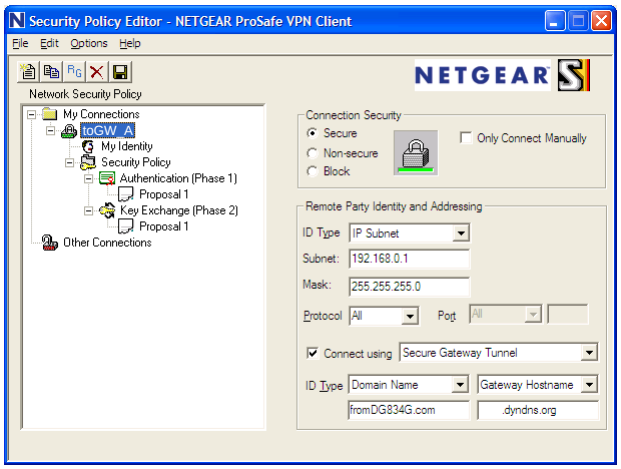
The PC needs to have a VPN client program installed that supports IPSec (in this case study, the NETGEAR VPN ProSafe Client is used). Go to the NETGEAR website (*www.netgear.com*) for information about how to purchase the NETGEAR ProSafe VPN Client.

**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 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, 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. Select **Secure** in the Connection Security section.

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

f. In this example, type **192.168.0.1** in the **Subnet** field as the network address of the modem router.

g. Enter **255.255.255.0** in the **Mask** field as the LAN subnet mask of the modem router.

h. Select **All** in the **Protocol** drop-down list to allow all traffic through the VPN tunnel.

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

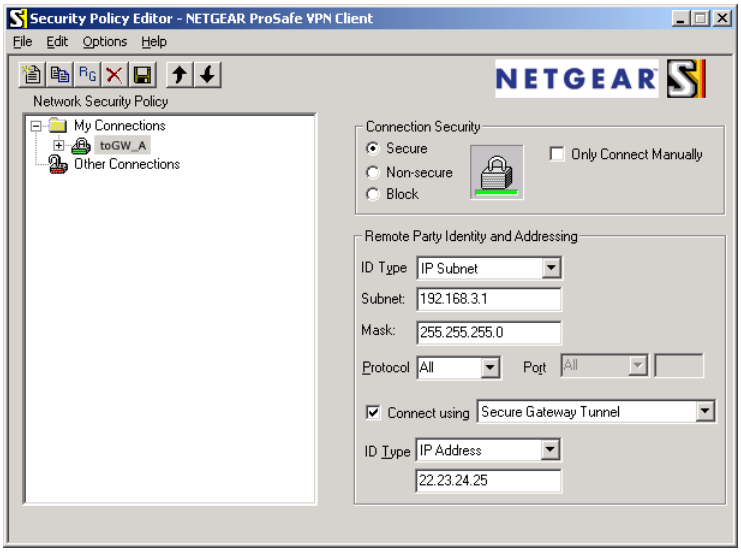
j. Select **Domain Name** in the **ID Type** drop-down list, and enter **fromGW_A.com** (in this example).

k. Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).

3. Configure the security policy in the 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.

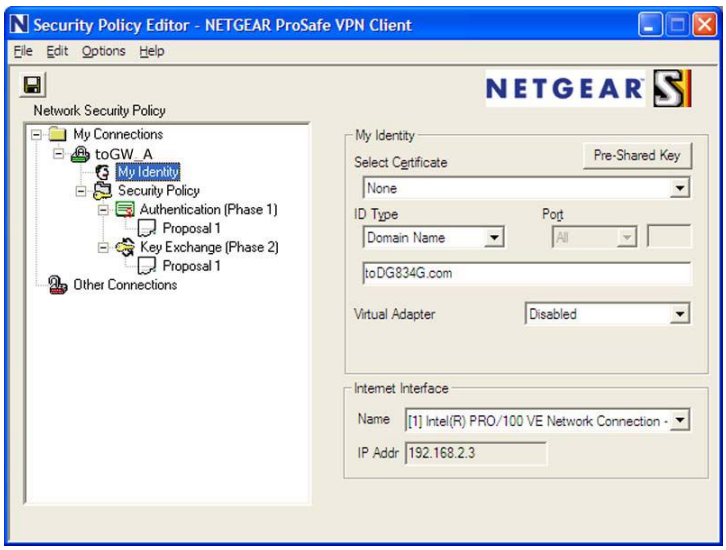



c. Select the **Main Mode** radio button in the Select Phase 1 Negotiation Mode group.

4. Configure the VPN client identity.

In this step, you provide information about the remote VPN client PC. You have to provide the pre-shared key that you configured in the 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. Select **None** in the **Select Certificate** field.

c. Select **Domain Name** in the **ID Type** field, and enter **toGW_A.com** (in this example). Select **Disabled** in the **Virtual Adapter** field.

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

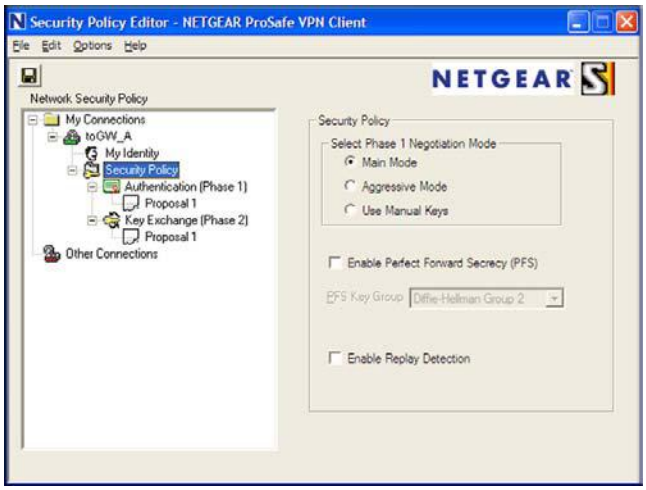
e. Click the **Pre-Shared Key** button.

f. In the Pre-Shared Key screen, click **Enter Key**. Enter the DGN2200'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 has to 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**.

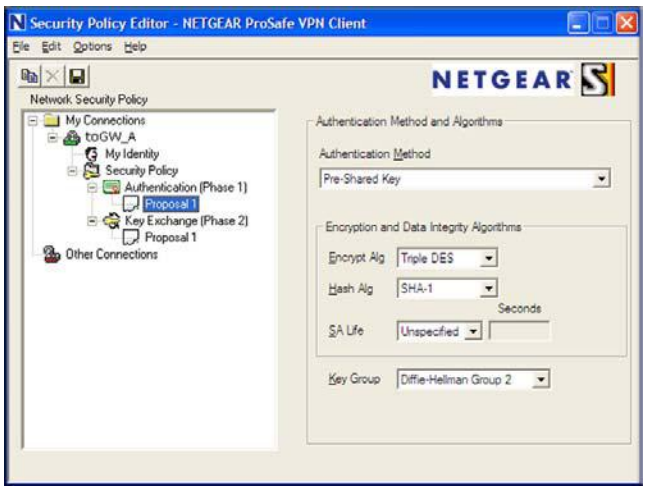
e. In the **Hash Alg** drop-down list, select **SHA-1**.

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 has to 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 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 has to 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 toDGN2200.

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


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

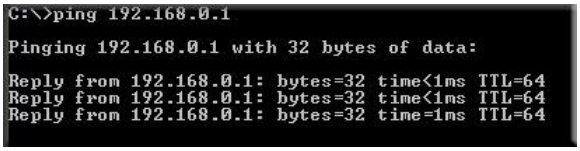
To perform a ping test using this example, start from the remote PC:

**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`**.




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

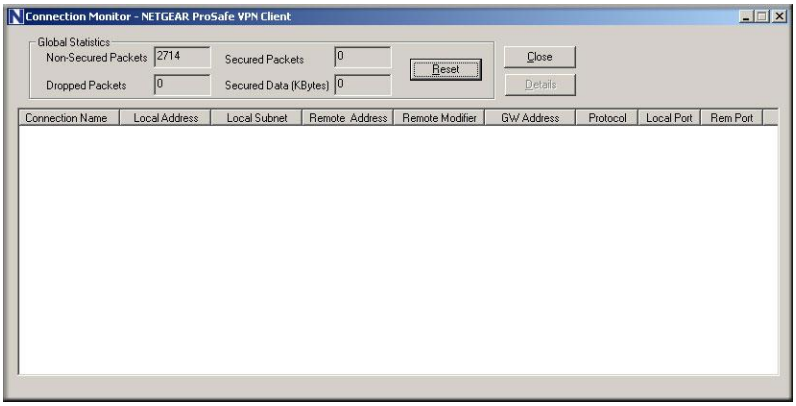
**Note:** You can use the VPN router diagnostics to test the VPN connection from the VPN router to the client PC. To do this, select Diagnostics on the modem router main menu.

# Monitoring the VPN Tunnel (Telecommuter Example)

To view information about the progress and status of the VPN client connection, open the Log Viewer. In Windows, click **Start**, and select Programs > N300 Wireless ADSL2+ Modem Router DGN2200 > 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:



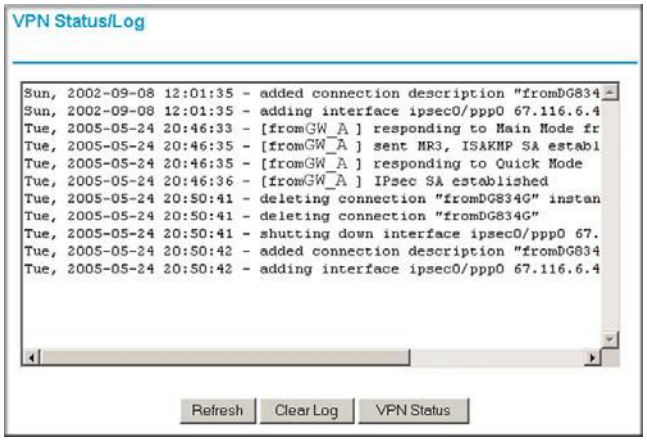
While the connection is being established, the connection name listed in this screen shows SA before the name of the connection. When the connection is successful, the SA changes to the yellow key symbol.

**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.

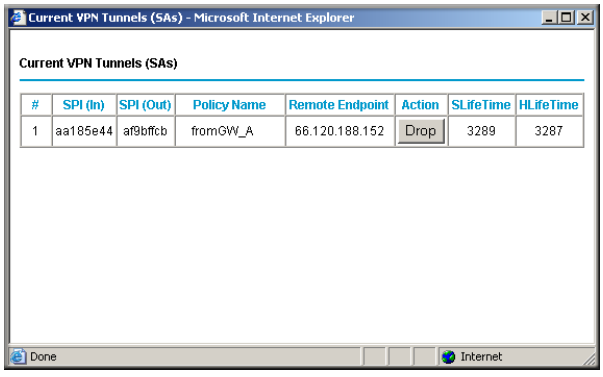
## Viewing the VPN Router's VPN Status and Log Information

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

1. On the 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

## Wireless Routers, Gateways, and Access Points

C

### Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

### FCC Requirements for Operation in the United States

#### FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

#### FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

#### FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, Santa Clara, CA 95134, declare under our sole responsibility that the model N300 Wireless ADSL2+ Modem Router DGN2200 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

#### FCC Radio Frequency Interference Warnings & Instructions

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

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

### FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

## Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N300 Wireless ADSL2+ Modem Router DGN2200) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

## Interference Reduction Table

**Table 14.**

| Household Appliance | Recommended Minimum Distance between NETGEAR equipment and household appliance to reduce interference (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 |

## Europe – EU Declaration of Conformity

Marking with the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC).

This equipment meets the following conformance standards:

- EN300 328 (2.4 Ghz), EN301 489-17, EN301 893 (5 Ghz), EN60950-1
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.
- In Italy, the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.
- This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.
- For complete DoC, visit the NETGEAR EU Declarations of Conformity website at: *http://kb.netgear.com/app/answers/detail/a_id/11621/*
- For GNU General Public License (GPL) related information, please visit *http://kbserver.netgear.com/kb_web_files/open_src.asp*

## EDOC in Languages of the European Community

| | |
|---|---|
| Cesky [Czech] | *NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES. |
| Dansk [Danish] | Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. |
| Deutsch [German] | Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet. |
| Eesti [Estonian] | Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. |
| English | Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. |
| Español [Spanish] | Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE. |
| Ελληνική [Greek] | ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ. |
| Français [French] | Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. |
| Italiano [Italian] | Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE. |
| Latviski [Latvian] | Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. |
| Lietuvių [Lithuanian] | Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas. |
| Nederlands [Dutch] | Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. |
| Malti [Maltese] | Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC. |
| Magyar [Hungarian] | Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak. |
| Polski [Polish] | Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC. |

| | |
|---|---|
| Português [Portuguese] | *NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE. |
| Slovensko [Slovenian] | NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES. |
| Slovensky [Slovak] | *NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES. |
| Suomi [Finnish] | *NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
| Svenska [Swedish] | Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG. |
| Íslenska [Icelandic] | Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC. |
| Norsk [Norwegian] | *NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF. |

# Index

## G



## H



## I



## K



## L



## M



## N

## O



## P



## Q



## R



## S



## T

## U



## V



## W