N300 Wireless ADSL2+ Modem Router
DGN2200Mv2
User Manual
Technical Support
Thank you for choosing NETGEAR. For support information and firmware upgrades, please visit:
http://www.hcom.co.za.
For more information about the topics covered in this manual, visit the Support website at
Modem support: 0860 266 344
Support hours are Monday to Friday: 08h00 to 17h00
Telkom ADSL support: 10210

Trademarks
NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of
NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change
without notice. Other brand and product names are registered trademarks or trademarks of their respective
holders. © 2011 NETGEAR, Inc. All rights reserved.

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.
# Table of Contents

## Chapter 1  Internet Configuration

- Log In. ................................................. 7
- Setup Wizard ........................................ 8
- Fixed IP (Static) Account Setup. .................... 10
- Manual Setup ....................................... 10
  - Broadband Settings .................................. 10
  - 3G Mobile Broadband Settings .................... 12
  - Basic ISP Settings .................................. 13
  - ADSL Settings ...................................... 16

## Chapter 2  Wireless Network Configuration

- Preset Wireless Security ............................. 19
- Plan Your Wireless Network ......................... 19
  - Wireless Placement and Range Guidelines ........ 20
  - Wireless Security Options ......................... 20
- Manually Configure Wireless Settings .............. 22
  - Restrict Access by MAC Address ................. 24
  - WPA, WPA2, or WPA + WPA2 ....................... 26
  - WEP .............................................. 26
- Push 'N' Connect (WPS) Method ...................... 28
  - WPS Button ....................................... 28
  - WPS PIN Entry .................................... 30
  - Add Devices That Do Not Support WPS .......... 30

## Chapter 3  Protect Your Network

- Password and Login Timeout Settings ............. 33
  - Change the Built-In Password .................... 33
  - Change the Administrator Login Time-Out ....... 34
- Block Keywords, Sites, and Services ............... 34
  - Blocking Sites .................................... 34
  - Block Services .................................... 35
- Firewall Rules ..................................... 36
- Time Zones and Services Scheduling ............... 37
  - Set Your Time Zone ............................... 38
  - Schedule Firewall Services ...................... 38
- View, Select, and Save Logged Information ........ 39
  - Log Message Examples ............................ 40
  - Enable Security Event Email Notification ....... 40
Chapter 4 Manage Your Network

Back Up, Restore, and Erase Your Settings .............................................. 44
Router Status and Usage Statistics .......................................................... 45
Statistics ....................................................................................................... 47
Connection Status ...................................................................................... 49
Attached Devices ....................................................................................... 50
Diagnostics and Rebooting .......................................................................... 50
Remote Management ................................................................................... 51

Chapter 5 Advanced Configuration

WAN Settings ............................................................................................. 54
Default DMZ Server ................................................................................... 55
Dynamic DNS ............................................................................................... 56
LAN Settings ............................................................................................... 57
   DHCP ........................................................................................................ 58
       Reserved IP Addresses .................................................................... 59
Quality of Service (QoS) ............................................................................ 60
Advanced Wireless Settings ........................................................................ 62
Static Routes ............................................................................................... 63
Universal Plug and Play ............................................................................. 65
TR069 Client Configuration ........................................................................ 66
Wireless Bridging and Repeating Networks ................................................ 67
   Point-to-Point Bridge Configuration ....................................................... 68
   Multi-Point Bridge ............................................................................... 69
   Repeater with Wireless Client Association ......................................... 70

Chapter 6 VPN Lite

Configuring VPN Lite Sites ......................................................................... 73

Chapter 7 Troubleshooting

Basic Functioning ........................................................................................ 76
   Welcome Screen Displays instead of Router Main Menu ...................... 76
Troubleshooting with the LEDs .................................................................. 76
Cannot Log In to the Wireless Modem Router ......................................... 78
Troubleshooting the Internet Connection ................................................... 78
   ADSL Link ............................................................................................. 78
   Internet LED Is Red ............................................................................. 79
Obtaining an Internet IP Address ............................................................... 80
Troubleshooting PPPoE or PPPoA ............................................................... 80
Troubleshooting Internet Browsing ............................................................. 81
Troubleshooting a TCP/IP Network Using the Ping Utility ....................... 81
   Testing the LAN Path to Your Wireless Modem Router ....................... 81
   Testing the Path from Your Computer to a Remote Device ................. 82
Restoring the Default Configuration and Password ............................... 83
   Using the Restore Factory Settings Button to Reset the Router .......... 83
Problems with Date and Time ........................................... 83

Appendix A  Technical Specifications

Technical Specifications .................................................. 85
Telkom Factory Default Configuration ............................... 86

Appendix B  Notification of Compliance

Index
Internet Configuration

This chapter describes how to configure your N300 Modem Router Internet connection. This chapter includes:

- Log In
- Setup Wizard
- Fixed IP (Static) Account Setup
- Manual Setup

For help with installation and initial setup, see the N300 Modem Router DGN2200Mv2 Installation Guide included in the package, or use the Animated Install Guide on the CD. For installation instructions in a language other than English, see the language options on the CD.

For more information about the topics covered in this manual, visit the support website at http://support.netgear.com.
Log In

You can log in to the wireless modem router to view or change its settings, and to access the Knowledge Base and documentation.

When you have logged in, if you do not click Logout, the wireless modem router waits for 5 minutes after no activity before it automatically logs you out.

➢ To log in to the wireless modem router:

1. If you have not set up wireless connections yet, connect your computer to the wireless modem router with an Ethernet cable.

2. In the address field of your Internet browser, type http://www.routerlogin.com.

   To connect, you can also enter the modem router’s IP address, http://10.0.0.2.

   The wireless modem router user name and password are not the same as any other user name or password you might use to log in to your Internet connection.

3. Enter admin for the user name and your password (or the default, admin).

   For information about how to change the password, see Change the Built-In Password on page 33.

4. The screen that displays when you log in depends on whether the wireless modem router has already been set up.
   • Smart Wizard screen: The wireless modem router has never been configured. You can use the Setup Wizard to automatically detect your Internet connection (see Setup Wizard on page 8), or you can bypass the Setup Wizard and manually configure your Internet connection (see Basic ISP Settings on page 13).
   • Router Status screen: The wireless modem router Internet connection is not configured, or the wireless modem router has been reset to its factory default settings. See Router Status and Usage Statistics on page 45.
Setup Wizard

The Setup Wizard can check your Internet connection for servers and protocols to determine your ISP configuration. You can also manually specify your Internet connection settings in the Setup Wizard Basic Settings screen. For instructions on manually configuring your 3G Mobile Broadband settings, see 3G Mobile Broadband Settings on page 12.

**Note:** NETGEAR recommends that you use the installation CD-ROM to install and configure your NETGEAR wireless modem router, rather than using the firmware application to perform the installation. This will simplify the installation process, and ensure that your router is configured correctly.

➢ **To use the Setup Wizard:**

1. Select **Setup Wizard** to display the Setup Wizard Welcome screen.

![Figure 1. Setup Wizard Welcome Screen](image)

2. Click **Next** to display the following screen:

![Figure 2. 3G Mobile Broadband Settings Configuration Screen](image)

3. Select your Internet connection mode from the drop down menu.
Select one of the following:

- Use ADSL connection first and if fail 3G Mobile Broadband connection.
- Always use Mobile Broadband connection.
- Always use ADSL connection.

4. Click **Next** to display the following screen.

![Setup Wizard](image)

5. Click **Next**. Initially, a connection detection progress screen displays. When the router successfully detects the connection, additional screens display.
   
a. Enter your Internet service provider (ISP) configuration information. Select your country and your Internet service provider. If login credentials are required by your ISP, enter your user name and password. Click **Next**.

   b. Depending on the type of connection detected, you are prompted to enter your ISP settings. These may be one of the following:
      
      - **PPPoE or PPPoA**: This displays the PPPoE configuration screen. Enter the login user name and password. These fields are case-sensitive.
      - **Dynamic IP account setup**: No entries are necessary.
      - **IP over ATM Classical IP assignment (RFC1577)**: Enter the assigned IP address, subnet mask, and the IP address of the primary DNS server for your ISP. If a secondary DNS server address is available, enter that also. DNS servers translate an Internet name such as `www.netgear.com` to a numeric IP address.
      - **To configure a static IP address**: For instructions, see *Fixed IP (Static) Account Setup* on page 10.

6. At the end of the Setup Wizard, click **Test** to check your Internet connection.

   **Note**: If you have trouble connecting to the Internet, see *Chapter 7, Troubleshooting* for help.

7. After the test succeeds, click **Apply** to apply and save your configuration settings.
Fixed IP (Static) Account Setup

1. Select Basic Settings from the router menu.
2. If required, enter the account name and domain name from your ISP.
3. Select Use Static IP Address or Use IP Over ATM (IPoA — RFC1483 Routed) according to the information from your ISP. If you select IPoA, the router will detect the gateway IP address, but you still need to provide the router IP address.
4. Enter your assigned IP address, subnet mask, and the IP address of your ISP’s gateway wireless modem router. This information should have been provided to you by your ISP.
5. Enter the IP address of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it also. DNS servers translate an Internet name such as www.netgear.com to a numeric IP address.

Manual Setup

In order to connect to the network, an active broadband service account is required. Contact your ISP for your user name, password, and the network name. You must also configure some or all of the settings described in the following sections, depending on how you have chosen to connect to the Internet:

- Broadband Settings
- 3G Mobile Broadband Settings
- Basic ISP Settings
- ADSL Settings

The following sections provide instructions for each of these procedures.

Broadband Settings

➢ To configure your broadband Internet settings manually:

1. Select Broadband Settings.
This opens the Broadband Settings configuration screen, which allows you to configure your broadband settings, as shown in Figure 3, Broadband Settings Configuration Screen.

Figure 3. Broadband Settings Configuration Screen

2. Enter your settings.

Table 1 on page 12 describes the Broadband Settings fields and options.
3. Click **Apply** to apply and save your changes, or **Cancel** to discard your changes.

### Table 1. Broadband Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Connection Mode</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Use ADSL first and if fail use Mobile Broadband connection</td>
</tr>
<tr>
<td></td>
<td>• Always use Mobile Broadband connection</td>
</tr>
<tr>
<td></td>
<td>• Always use ADSL connection</td>
</tr>
<tr>
<td>Failover Detection Method¹</td>
<td>Select the failover method and enter the following information:</td>
</tr>
<tr>
<td></td>
<td>• DNS lookup using WAN DNS Server</td>
</tr>
<tr>
<td></td>
<td>• Perform a DNS lookup by a hostname</td>
</tr>
<tr>
<td></td>
<td>If you select this option, you must also enter the DNS lookup hostname in</td>
</tr>
<tr>
<td></td>
<td>the text field to the far right of this option.</td>
</tr>
<tr>
<td></td>
<td>• Ping this IP address</td>
</tr>
<tr>
<td></td>
<td>If you select this option, you must also enter the IP address in the</td>
</tr>
<tr>
<td></td>
<td>text field to the far right of this option.</td>
</tr>
<tr>
<td>Retry Interval is¹</td>
<td>Enter the retry interval in seconds.</td>
</tr>
<tr>
<td>Failover after¹</td>
<td>Enter the number of retry attempts to perform before failing over.</td>
</tr>
<tr>
<td>Resume after¹</td>
<td>Enter how long to wait for primary link to be stabilized before resuming</td>
</tr>
<tr>
<td></td>
<td>use of the primary link.</td>
</tr>
<tr>
<td>Enable Hardware link detection (Checkbox and</td>
<td>To enable, select the checkbox and enter the amount of time in seconds to</td>
</tr>
<tr>
<td>text field)</td>
<td>wait before failing over if the Ethernet link is dropped. This</td>
</tr>
<tr>
<td></td>
<td>is independent of the DNS/Ping detection methods.</td>
</tr>
</tbody>
</table>

¹. This field is available only when the **Internet Connection Mode** is **Use Ethernet first and if fail use 3G mobile connection**.

### 3G Mobile Broadband Settings

➢ **To configure your 3G mobile broadband Internet settings manually:**

1. Select **3G Mobile Broadband Settings**.

   This opens the 3G Mobile Broadband Settings configuration screen. This screen allows you to configure the broadband account access for your NETGEAR Modem.

![Figure 4. 3G Mobile Broadband Settings Configuration Screen](image)
2. Enter your settings. In order to connect to the network, an active broadband service account is Required. Contact your ISP for username, password, and the network name
   • **Username.** Account login username.
   • **Password.** Account password for authentication.
   • **Connect automatically at startup.** If selected, the modem will automatically connect to the network upon powered up. This should be selected after login information is provided.
   • **Reconnect automatically when connection is lost.** If selected, the modem will attempt to reconnect to the network when the connection is lost. Under normal situation, this setting should be selected.
   • **Roaming automatically.** If checked, it may roam to any available operator in range and may incur roaming charges.
   • **Connection Status.** Current WAN port status.

3. When done, select any of the following:
   • Click **Connect** when you want to manually connect to the network.
   • Click **Disconnect** when you want to manually disconnect from current network.
   • Click **Apply** when you finish changing the settings.
   • Click **Cancel** to discard changes.
   • Click **Refresh** to update connection status

**Basic ISP Settings**

➢ **To configure the basic settings manually:**

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

**ISP does not require login**

- **Yes**. If your ISP requires a login, select this radio button.
- **No**. If your ISP does not require a login, enter the account name, if required, and the domain name, if required.

3. Enter the settings for the IP address and DNS server. If you enter or change a DNS address, restart the computers on your network so that these settings take effect.

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

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

6. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within 1 minute, see *Troubleshooting the Internet Connection* on page 78.

When your Internet connection is working, you do not need to launch the ISP’s login program on your computer to access the Internet. When you start an Internet application, your wireless modem router automatically logs you in.
The following table describes the Basic Settings screen fields and options.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does Your ISP Require a Login?</td>
<td>• Yes&lt;br&gt;• No&lt;br&gt;These fields appear only if no login is required.</td>
</tr>
<tr>
<td>Account Name (If required)</td>
<td>Enter the account name provided by your ISP. This might also be called the host name.</td>
</tr>
<tr>
<td>Domain Name (If required)</td>
<td>Enter the domain name provided by your ISP.</td>
</tr>
<tr>
<td>Login</td>
<td>The login name provided by your ISP. This is often an e-mail address.</td>
</tr>
<tr>
<td>Password</td>
<td>The password that you use to log in to your ISP.</td>
</tr>
<tr>
<td>Service Name</td>
<td>If your ISP provided a service name, enter it here.</td>
</tr>
<tr>
<td>Idle Timeout (In minutes)</td>
<td>If you want to change the Internet login time-out, enter a new value in minutes. This determines how long the wireless modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of 0 (zero) means never log out.</td>
</tr>
<tr>
<td>Internet IP Address</td>
<td>• Get Dynamically from ISP. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.&lt;br&gt;• Use Static IP Address. Enter the IP address that your ISP assigned. Also enter the IP subnet mask and the gateway IP address. The gateway is the ISP’s wireless modem router to which your wireless modem router will connect.&lt;br&gt;• Use IP Over ATM (PoA). This option is available only if your ISP does not require a log in.</td>
</tr>
<tr>
<td>Domain Name Server (DNS) Address</td>
<td>The DNS server is used to look up site addresses based on their names.&lt;br&gt;• Get Automatically from ISP. Your ISP uses DHCP to assign your DNS server address automatically.&lt;br&gt;• Use These DNS Servers. If you know your ISP does not automatically transmit DNS addresses to the wireless 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.</td>
</tr>
</tbody>
</table>
### ADSL Settings

For information about how to install ADSL filters, see the Setup Manual.

NETGEAR recommends that you use the Setup Wizard to automatically detect and configure your ADSL settings. This usually works fine. However, if you have technical experience and are sure of the multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI), you can specify those settings here.

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

### Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT (Network Address Translation)</td>
<td>NAT automatically assigns private IP addresses (10.0.0.x) to devices on your LAN.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>. Usually NAT is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable</strong>. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure that you do not require it. When NAT is disabled, only classical routing is performed by this router. Classical routing lets you directly manage the IP addresses that the wireless modem router uses. Classical routing should be selected only by experienced users.¹</td>
</tr>
<tr>
<td></td>
<td>• Advanced users can also bridge or disable the firewall.</td>
</tr>
<tr>
<td>Router MAC Address</td>
<td>Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use Default MAC Address</strong>. This is the usual setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use Computer MAC address</strong>. If your ISP requires MAC authentication, you can use this setting to disguise the wireless modem router's MAC address with the computer's own MAC address.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use This MAC Address</strong>. If your ISP requires MAC authentication, you can manually type the MAC address for a different computer. The format for the MAC address is XX:XX:XX:XX:XX:XX.</td>
</tr>
</tbody>
</table>

¹. Use the Setup Wizard to select the correct country to optimize detection of the ADSL settings.
To specify ADSL settings manually:

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

![ADSL Settings screen](image)

If your ISP provided you with a multiplexing method or VPI/VCI number, then enter the setting. Otherwise, the default settings are adequate.

2. In the **Multiplexing Method** drop-down list, select **LLC-based** or **VC-based**.
   - For the VPI, type a number between 0 and 255. The default is 8.
   - For the VCI, type a number between 32 and 65535. The default is 35.

3. Click **Apply**.
Wireless Network Configuration

For a wireless connection, the SSID, also called the wireless network name, and the wireless security settings must be the same for the wireless modem router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.

**Note:** Computers can connect wirelessly at a range of hundreds of meters. If you do not use wireless security, this can allow others outside your immediate area to access your network.
Preset Wireless Security

The wireless 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 20.

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.

For information on how to connect additional devices to your wireless network, see *Push 'N' Connect (WPS) Method* on page 28.

Plan Your Wireless Network

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

To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.

To manually configure the wireless settings, have the following information on hand:

- SSID. The default SSID for the wireless modem router is printed on the label on the bottom of the unit.
- The wireless mode (80.211n, 802.11g, or 802.11b) that each wireless adapter supports.
- Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

See *Manually Configure Wireless Settings* on page 22.
• Push 'N' Connect (WPS) implements WPA/WPA2 wireless security on the wireless modem router and your wireless computer or device at the same time. The wireless computer or device must be compatible with WPS.

See Push 'N' Connect (WPS) Method on page 28.

Wireless Placement and Range Guidelines

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

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

• Near the center of the area in which your PCs will operate.
• In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
• Away from sources of interference, such as PCs, microwave ovens, and 2.4 GHz cordless phones.
• Away from large metal surfaces.
• Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.
• If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

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

Wireless Security Options

Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 100 meters (300 feet). Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The N300 Modem Router provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

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

• **Restrict access based on MAC address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the wireless modem router. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
• **Turn off the broadcast of the wireless network name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network discovery feature of some products, such as Windows XP, but the data is still exposed.

• **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK. WEP encryption is available only when the Mode setting is Up to 54 Mbps.

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

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

**Note:** If you use a wireless computer to change the wireless network name (SSID) or wireless security, you will be disconnected when you click **Apply**. To avoid this problem, connect your computer to the router with an Ethernet cable while you are making changes.

➢ **To view or manually configure the wireless settings:**

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

![Wireless Settings Screen]

**Note:** South Africa falls under the Europe region for Wi-Fi.

The settings for this screen are explained in **Table 2**.

2. Select the region in which the wireless modem router will operate.
3. For initial configuration and test, leave the other settings unchanged.
4. To save your changes, click **Apply**.
5. Configure and test your computers for wireless connectivity.

Set up your wireless computers with the same SSID and wireless security settings as your wireless modem router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the wireless modem router. If there is interference, adjust the channel.
### Table 2. Wireless Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network Name (SSID)</td>
<td>The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. When there is more than one wireless network, SSIDs provide a means for separating the traffic. To join a network, a wireless computer or device must use the SSID.</td>
</tr>
<tr>
<td>Region</td>
<td>The location where the wireless modem router is used. South Africa falls under the Europe region for Wi-Fi.</td>
</tr>
</tbody>
</table>
| Channel                | The wireless channel: 1 through 13. This setting applies to any guest networks you set up. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to try different channels to see which is best. The number of available channels varies by region and depends on the selected mode.  
  - For Up to 145 Mbps mode, the default channel is 11.  
  - For Up to 300 Mbps mode, the default channel is 7. |
| Mode                   | The mode can be set only for the primary wireless LAN (NETGEAR).                                                                                                                                               |
|                        | **Up to 300Mbps:** This is the fastest mode, and is compatible with all 802.11g, 802.11b, and faster Draft-N wireless stations. The channel bandwidth expands from 20 MHz to 40 MHz to achieve the 300 Mbps rate. Channel expansion operates on a frame-by-frame basis to avoid interference with transmissions from other wireless networks. Two channels are used, but only the first is listed in the Channel field. The associated channels are: 1+5, 2+6, 3+7, 4+8, 5+9, 6+10, and 7+11.  
  **Note.** WPA-PSK, WPA2-PSK (AES), or WPA-PSK (TKIP) + WPA2-PSK (AES) security is required for the Up to 300 Mbps Mode setting.  
|                        | **Up to 145Mbps** (default setting): Allows wireless stations that support speeds up to 134 Mbps. The router transmits two streams with different data concurrently on the same channel. This mode restricts channel bandwidth to minimize interference with the transmissions of other wireless networks.  
  **Note.** WPA-PSK, WPA2-PSK (AES), or WPA-PSK (TKIP) + WPA2-PSK (AES) security is required for the Up to 145 Mbps Mode setting.  
|                        | **Up to 54 Mbps:** Allows wireless stations that support speeds up to 54 Mbps.                                                                                                                                  |
| Enable this Wireless Network | You can completely turn off the wireless connectivity of the wireless modem router by pressing the Wireless On/Off button on the front panel of the wireless modem router. For example, if you use your notebook computer to wirelessly connect to your wireless modem router and you take a business trip, you can turn off the wireless portion of the wireless modem router while you are traveling. Other members of your household who use computers connected to the wireless modem router through Ethernet cables can still use the wireless modem router. To do this, clear the Enable Wireless Access Point check box on the Wireless Settings screen, and then click Apply. |
Restrict Access by MAC Address

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the wireless modem router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. The Wireless Card Access List determines which wireless hardware devices will be allowed to connect to the wireless modem router.

Table 2. Wireless Settings (Continued)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSID Broadcast</td>
<td>By default, the wireless modem router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To do this, clear the Allow Broadcast of Name (SSID) check box on the Wireless Settings screen, and then click Apply. Wireless devices will not “see” your wireless modem router. You must configure your wireless devices to match the wireless network name (SSID) of the wireless modem router. The SSID of any wireless access adapters must match the SSID you specify in the wireless modem router. If they do not match, you will not get a wireless connection to the wireless modem router.</td>
</tr>
<tr>
<td>Enable Wireless Isolation</td>
<td>If checked, the wireless client under this SSID can access only the Internet and can’t access other wireless clients even under the same SSID, Ethernet clients, or this device. Other clients can’t access the wireless client, either.</td>
</tr>
<tr>
<td>Security Options</td>
<td>None</td>
</tr>
<tr>
<td>WEP</td>
<td>Use encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. See WEP. WEP is available only when the Mode setting is Up to 54 Mbps.</td>
</tr>
<tr>
<td>WPA-PSK (TKIP)</td>
<td>Allow only computers configured with WPA to connect to the wireless modem router. See WPA, WPA2, or WPA + WPA2.</td>
</tr>
<tr>
<td>WPA2-PSK (AES)</td>
<td>Allow only computers configured with WPA2 to connect to the wireless modem router. See WPA, WPA2, or WPA + WPA2.</td>
</tr>
<tr>
<td>WPA-PSK (TKIP) + WPA2-PSK (AES)</td>
<td>Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless modem router. See WPA, WPA2, or WPA + WPA2.</td>
</tr>
</tbody>
</table>
To restrict access based on MAC addresses:

1. Select **Setup > Wireless Settings** and click the **Set Up Access List** button to display the list.

2. Select the **Turn Access Control On** check box to enable the restricting of wireless computers by their MAC addresses.

   **Note:** If you are using a wireless connection, do not click **Apply** until you have added your computer’s MAC address in this screen.

3. Use the **Add** button to add wireless stations so that they will have access.

   - You can select currently connected wireless computers from the Available Wireless Cards List.
   - You can type in the MAC address for the wireless computer or device. The MAC address is usually printed on the wireless card, or on the label of a wireless device. It might appear in the wireless modem router’s DHCP table. The MAC address is 12 hexadecimal digits.
   - You can copy and paste the MAC addresses from the wireless modem router’s Attached Devices screen into the MAC Address field of this screen. To do this, configure each wireless computer to obtain a wireless link to the wireless modem router. The computer should then appear in the Attached Devices screen.

4. Click **Add** to add each entry. You can add several stations to the list.

5. When you are finished adding stations, click **Apply**.

Now, only computers and devices on this list can wirelessly connect to the wireless modem router. This prevents unauthorized access to your network.
Wireless Network Configuration

WPA, WPA2, or WPA + WPA2

**Note:** WPA-PSK, WPA2-PSK (AES), or WPA-PSK (TKIP) + WPA2-PSK (AES) security is required for the Up to 145 Mbps or Up to 300 Mbps Mode setting.

Both WPA and WPA2 provide strong data security. WPA with TKIP is a software implementation that can be used on Windows systems with Service Pack 2 or later, WPA2 with AES is a hardware implementation; see your device documentation before implementing it. Consult the product documentation for your wireless adapter for instructions for configuring WPA settings.

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

➢ **To configure WPA or WPA2 in the wireless modem router:**

1. Select **Wireless Settings**.
2. Select the radio button for the WPA or WPA2 option of your choice. The settings displayed on the screen depend on which security option you select.
3. For WPA-PSK or WPA2-PSK, enter the passphrase.
4. To save your settings, click **Apply**.

**WEP**

WEP encryption is available only when the Mode setting is Up to 54 Mbps.

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

1. Select **Wireless Settings** to display the following screen. Make sure the Mode setting is set to **Up to 54 Mbps**.
2. In the Security Options section, select the **WEP** radio button:

   ![Wireless Settings](image)

3. Select the **Authentication Type**: **Automatic** or **Shared Key**. The default is Automatic.

   *Note: The authentication is separate from the data encryption. You can select authentication that requires a shared key, but still leaves data transmissions unencrypted. Security is stronger if you use both the Shared Key and WEP encryption settings.*

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

5. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network:
   - **Passphrase**. To use a passphrase to generate the keys, enter a passphrase, and click **Generate**. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the wireless modem router.
Note: Not all wireless adapters support passphrase key generation.

- **Key 1–Key 4.** These values are not case-sensitive. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits for 64 bit encryption or 26 digits for 128-bit encryption (any combination of 0–9, a–f, or A–F).

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

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

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

**Push 'N' Connect (WPS) Method**

For you to use Push 'N' Connect, your wireless computers or devices must support Wi-Fi Protected Setup (WPS). Compatible equipment usually has the WPS symbol on it. WPS can configure the network name (SSID) and set up WPA/WPA2 wireless security for the wireless modem router and the wireless computer or device at the same time.

Some considerations regarding WPS are:

- NETGEAR's Push 'N' Connect feature is based on the WPS standard. All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.
- If your wireless network will include a combination of WPS-capable devices and non-WPS-capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding WPS-capable devices.

You can connect to the network using WPS either with a push button or a PIN.

- **Push Button.** This is the preferred method. See the following section, *WPS Button*.
- **Entering a PIN.** See *WPS PIN Entry* on page 30.

**WPS Button**

Any wireless computer or wireless adapter that will connect to the wireless modem router wirelessly is a client. The client must support a WPS button, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.
To use the wireless modem router WPS button to add a WPS client:

1. Select Add a WPS Client and click Next.
   
   By default, the Push Button (recommended) radio button is selected.

2. Either click the onscreen button or press the WPS button on the front of the wireless modem router.

   The wireless modem router tries to communicate with the client (the computer that wants to join the network) for 2 minutes.

3. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility’s instructions to click a WPS button.

4. Go back to the wireless modem router screen to check for a message.

   The wireless modem router WPS screen displays a message confirming that the client was added to the wireless network. The wireless modem router generates an SSID, and implements WPA/WPA2 wireless security. The wireless modem router keeps these wireless settings unless you change them, or you clear the Keep Existing Wireless Settings check box in the WPS Settings screen.

   Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See Manually Configure Wireless Settings on page 22.

To access the Internet from any computer connected to your wireless modem router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the wireless modem router’s Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute time frame, the SSID does not change, and no security is implemented on the wireless modem router.
WPS PIN Entry

Any wireless computer or device that will connect to the wireless modem router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

The first time you add a WPS client, make sure that the **Keep Existing Wireless Settings** check box on the WPS Settings screen is cleared. This is the default setting for the wireless modem router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the wireless modem router automatically selects this check box so that your SSID and wireless security settings stay the same if other WPS devices are added later.

To use a PIN to add a WPS client:

1. Select **Add a WPS Client** (computers that will connect wirelessly to the wireless modem router are clients), and then click **Next**. The Add WPS Client screen displays:

2. Select the **PIN Number** radio button.

3. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility’s instructions to generate a PIN. Take note of the client PIN.

4. Enter the client PIN number and click **Next**.
   - The wireless modem router tries to communicate with the client for 4 minutes.
   - The wireless modem router WPS screen confirms that the client was added to the wireless network. The wireless modem router generates an SSID, and implements WPA/WPA2 wireless security.
   - If the client is not added during the 2-minute time frame, the router wireless settings remain unchanged.

5. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See **Manually Configure Wireless Settings** on page 22.

To access the Internet from any computer connected to your wireless modem router, launch an Internet browser. You should see the wireless modem router’s Internet LED blink, indicating communication to the ISP.

Add Devices That Do Not Support WPS

If you set up your network with WPS, and now you want to add a computer that does not support WPS, you must manually configure that computer. For information about how to view the wireless settings for the router, see **Manually Configure Wireless Settings** on page 22.

Because WPA randomly creates the SSID and WPA/WPA2 keys, they might be difficult to type or remember (that is one reason why the network is so secure). You can change the...
To change the network wireless settings:

Note: Making these changes causes all wireless computers to be disconnected from network. You then have to set them up with the new wireless settings.

1. Use an Ethernet cable to connect a computer to the router. That way you will not get disconnected when you change the wireless settings.

2. Log in to the router and select Wireless Settings (see Manually Configure Wireless Settings on page 22).

3. Make the following changes:
   - Change the wireless network name (SSID) to a meaningful name.
   - On the WPA/PSK + WPA2/PSK screen, select a passphrase.
   - Make sure that the Keep Wireless Settings check box is selected in the WPS Settings screen so that your new settings will not be erased if you use WPS.

4. Click Apply so that your changes take effect. Write down your settings.

   All wireless clients are disassociated and disconnected from the wireless modem router.

5. For the non-WPS devices that you want to connect, open the networking utility and follow the utility’s instructions to enter the security settings that you selected in Step 3 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).

6. For the WPS devices that you want to connect, follow the procedure in WPS Button on page 28 or WPS PIN Entry on page 30.

   The settings that you configured in Step 3 are broadcast to the WPS devices so that they can connect to the wireless modem router.
This chapter describes how to use the basic firewall features of the wireless modem router to protect your network. The chapter includes:

- Password and Login Timeout Settings
- Block Keywords, Sites, and Services on page 34
- Firewall Rules on page 36
- Time Zones and Services Scheduling on page 37
- Enable Security Event Email Notification on page 40
Password and Login Timeout Settings

For security reasons, the wireless modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the login automatically disconnects. You can use the following procedures to change the wireless modem router’s password and the period for the administrator’s login time-out.

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

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

Change the Built-In Password

➢ To change the built-in password:

1. Select **Maintenance > Set Password**.

![Set Password](image)

2. First enter the old password, and then enter the new password twice.
3. Click **Apply** to save your changes.

**Note:** After changing the password, you are required to log in again to continue the configuration. If you have backed up the wireless modem router settings previously, you should do a new backup so that the saved settings file includes the new password.
Change the Administrator Login Time-Out

For security, the administrator's login to the wireless modem router configuration times out after a period of inactivity.

➢ To change the login time-out period:

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

Block Keywords, Sites, and Services

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

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

Blocking Sites

➢ To block keywords and sites:

2. To enable keyword blocking, select one of the following:
   • **Per Schedule.** Turn on keyword blocking according to the settings in the Schedule screen.
   • **Always.** Turn on keyword blocking all the time, independent of the Schedule screen.
   • **Never.** Select never to turn off service blocking.

3. Enter a keyword or domain in the **Keyword** field, click **Add Keyword** and click **Apply**.
   Some examples of keyword application follow:
   • If the keyword XXX is specified, the URL http://www.badstuff.com/xxx.html is blocked.
   • If the keyword .com is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
   • Enter a period (.) to block all Internet browsing access.
   Up to 32 entries are supported in the Keyword list.

4. To delete a keyword or domain, select it from the list, click **Delete Keyword**, and then click **Apply**.

5. To specify a trusted user, enter that computer’s IP address in the **Trusted IP Address** field, and click **Apply**.
   You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.

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

**Block Services**

➢ **To block services:**

1. Select **Security > Services**.

2. Click **Add** and the following screen displays:

3. Either select a service from the **Service Type** drop-down list, or select **User Defined** to create a custom service.

4. Click **Add** to create the service, and the Service is listed in the Service Table.
5. Click **Apply** to save your settings.

## Firewall Rules

Use this screen to create firewall rules to block or allow specific traffic.

**Note:** This feature is for Advanced Administrators only. Incorrect configuration will cause serious problems.

➢ **To create firewall rules:**

1. **Select Security > Firewall Rules:**

2. **To create firewall rules for outbound services:**

   The table under Outbound Services lists all existing rules for outbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule allows all outgoing traffic.

   a. From the Firewall Rules screen under Outbound Services, click **Add**:

   b. Complete the Outbound Services screen, and save the data. The new rule will be listed in the table when you return to this screen.

3. **To create firewall rules for inbound services:**
The table under inbound services lists all existing rules for inbound traffic. If you have not defined any rules, only the default rule will be listed. The default rule blocks all inbound traffic.

**a.** From the Firewall Rules screen under Inbound Services, click **Add**:

![Inbound Services Table](image1)

**b.** Complete the Inbound Services screen, and save the data. The new rule will be listed in the table when you return to this screen.

4. To apply or cancel:

   **a.** Click **Apply** to update changes to the Outbound Services and Inbound Services tables.

   **b.** Click **Cancel** to disregard any unsaved changes.

### Time Zones and Services Scheduling

The wireless 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. On the router menu, select **Schedule** under Security to display the Security screen:

![Schedule Screen](image2)
Set Your Time Zone

To localize the time for your log entries, you must specify your time zone:

1. In the Schedule screen, select your time zone.
   This setting is used for the blocking schedule according to your local time zone and for time-stamping log entries.
2. If your time zone is currently in daylight savings time, select the Adjust for Daylight Savings Time check box.

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

3. The wireless modem router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, select the Use this NTP Server check box, and enter its IP address.
4. Click **Apply** to save your settings.

Schedule Firewall Services

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

To block Internet services based on a schedule:

1. From the Schedule screen, select Every Day or select one or more days.
2. 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, or enter times in the Start Time and End Time 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 will be effective through midnight the next day.

3. Click **Apply** to save your changes.
View, Select, and Save Logged Information

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

To view the log, select Security > Logs to display a screen similar to the following:

You can write the logs to a computer running a syslog program by selecting Broadcast on LAN or entering the IP address of the server where the syslog file will be written.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time</td>
<td>The date and time the log entry was recorded.</td>
</tr>
<tr>
<td>Description or action</td>
<td>The type of event and what action was taken, if any.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The IP address of the initiating device for this log entry.</td>
</tr>
<tr>
<td>Source port and interface</td>
<td>The service port number of the initiating device, and whether it originated from the LAN or WAN.</td>
</tr>
<tr>
<td>Destination</td>
<td>The name or IP address of the destination device or website.</td>
</tr>
<tr>
<td>Destination port and interface</td>
<td>The service port number of the destination device, and whether it is on the LAN or WAN.</td>
</tr>
</tbody>
</table>
Log Message Examples

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

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

Tue, 2006-05-21 18:55:00 - Administrator login successful-IP:10.0.0.2
Thu, 2006-05-21 18:56:58 - Administrator logout - IP:10.0.0.2
[This entry shows an administrator logging in and out from IP address 10.0.0.2.]

Tue, 2006-05-21 19:00:06 - Login screen timed out - IP:10.0.0.2
[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 e-mailed.]

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.]

Enable Security Event Email Notification

To receive logs and alerts by email, you must provide your email information in the E-mail screen and specify which alerts you would like to receive and how often.
In the main menu, under Security, select **E-mail**. The E-mail screen displays.

You can make the following selections:

- **Turn E-mail Notification On**. Select this check box if you want to receive email logs and alerts from the wireless modem router.

- **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 e-mail program. Enter the e-mail address to which logs and alerts are sent. This e-mail address is also used as the From address. If you leave this field blank, log and alert messages are not sent by e-mail.

- **Send to This E-mail Address**. 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 through email.

- **My Mail Server 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 e-mail account that is not provided by your ISP, select this field, and enter the required user name and password information.

- **Send E-Mail alerts immediately**. Select this check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.

- **Send logs according to this schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - **Day for sending log**. Specifies which day of the week to send the log. Relevant when the log is sent weekly.
  - **Time for sending log**. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

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

This chapter describes how to perform network management tasks with your wireless modem router. This chapter includes:

- Back Up, Restore, and Erase Your Settings
- Router Status and Usage Statistics
- Attached Devices
- Diagnostics and Rebooting
- Remote Management
Back Up, Restore, and Erase Your Settings

The configuration settings of the wireless modem router are stored in a configuration file. This file can be backed up to your computer, restored, or reverted to factory default settings. The following procedures explains how to do these tasks.

➢ To back up the configuration to a file

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

   ![Backup Settings Screen]

2. Click Save to save a copy of the current settings.
3. Store the .cfg file on a computer on your network.

➢ To restore the configuration from a file

1. Select Maintenance > Backup Settings.
2. Enter the full path to the file on your network or click the Browse button to locate the file.
3. When you have located the .cfg file, click the Restore button to upload the file to the wireless modem router. The wireless modem router then reboots automatically.

➢ To erase the Configuration

Select Maintenance > Backup Settings, and click the Erase button. The wireless modem router reboots and resets to the factory default settings.

After an erase, the wireless modem router’s password is admin, the LAN IP address is 10.0.0.2, and the wireless modem router’s DHCP client is enabled.

---

**Note:** To restore the factory default configuration settings when you do not know the login password or IP address, press the Restore Factory Settings button on the bottom of the wireless modem router for 6 seconds.
Router Status and Usage Statistics

Select Maintenance > Router Status.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>The host name assigned to the router in the Basic Settings screen.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>The wireless modem router firmware version.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ADSL Port MAC Address</td>
<td>The Ethernet MAC address being used by the Internet (ADSL) port.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address used by the Internet (ADSL) port. If no address is shown, the wireless modem router cannot connect to the Internet.</td>
</tr>
<tr>
<td>Network Type</td>
<td>The network type depends upon your ISP.</td>
</tr>
<tr>
<td>IP Subnet Mask</td>
<td>The IP subnet mask used by the Internet (ADSL) port.</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>IP address used as a gateway to the Internet for computers configured to use DHCP.</td>
</tr>
<tr>
<td>Domain Name Server</td>
<td>The DNS server IP addresses used by the wireless modem router. These addresses are usually obtained dynamically from the ISP.</td>
</tr>
<tr>
<td>PPPoE Session 2 IP Address</td>
<td></td>
</tr>
<tr>
<td>PPPoE Session 2 Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>PPPoE Session 2 Gateway IP address</td>
<td></td>
</tr>
<tr>
<td>LAN Port MAC Address</td>
<td>This field displays the Ethernet MAC address being used by the local (LAN) port of the wireless modem router.</td>
</tr>
<tr>
<td>IP Address</td>
<td>This field displays the IP address being used by the local (LAN) port of the wireless modem router. The default is 10.0.0.2.</td>
</tr>
<tr>
<td>DHCP</td>
<td>If Off, the wireless modem router does not assign IP addresses to PCs on the LAN. If On, the wireless modem router does assign IP addresses to PCs on the LAN.</td>
</tr>
<tr>
<td>IP Subnet Mask</td>
<td>This field displays the IP subnet mask being used by the local (LAN) port of the wireless modem router. The default is 255.255.255.0.</td>
</tr>
<tr>
<td>Modem ADSL Firmware Version</td>
<td>The version of the firmware.</td>
</tr>
<tr>
<td>Modem Status</td>
<td>The connection status of the modem.</td>
</tr>
<tr>
<td>DownStream Connection Speed</td>
<td>The speed at which the modem is receiving data from the ADSL line.</td>
</tr>
<tr>
<td>UpStream Connection Speed</td>
<td>The speed at which the modem is transmitting data to the ADSL line.</td>
</tr>
<tr>
<td>VPI</td>
<td>The Virtual Path Identifier setting.</td>
</tr>
<tr>
<td>VCI</td>
<td>The Virtual Channel Identifier setting.</td>
</tr>
</tbody>
</table>
Statistics

On the Router Status screen, click the Show Statistics button to display wireless modem router usage statistics, as shown in the following screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics</td>
<td></td>
</tr>
<tr>
<td>HSDPA Modem</td>
<td></td>
</tr>
<tr>
<td>Modem Identity</td>
<td></td>
</tr>
<tr>
<td>Modem SW</td>
<td></td>
</tr>
<tr>
<td>version</td>
<td></td>
</tr>
<tr>
<td>Modem driver</td>
<td></td>
</tr>
<tr>
<td>version</td>
<td></td>
</tr>
<tr>
<td>IMSI</td>
<td></td>
</tr>
<tr>
<td>IMEI</td>
<td></td>
</tr>
<tr>
<td>Operator</td>
<td></td>
</tr>
<tr>
<td>Network mode</td>
<td></td>
</tr>
<tr>
<td>Wireless Port</td>
<td></td>
</tr>
<tr>
<td>Name (SSID)</td>
<td>The service set ID, also known as the wireless network name for WLAN1.</td>
</tr>
<tr>
<td>Region</td>
<td>The country where the unit is set up for use.</td>
</tr>
<tr>
<td>Channel</td>
<td>The current channel, which determines the operating frequency.</td>
</tr>
<tr>
<td>Wireless AP</td>
<td>Indicates if the access point feature is enabled for WLAN1. If disabled,</td>
</tr>
<tr>
<td></td>
<td>the Wireless LED on the front panel is off.</td>
</tr>
<tr>
<td>Broadcast Name</td>
<td>Indicates if the wireless modem router is configured to broadcast its SSID</td>
</tr>
<tr>
<td></td>
<td>for WLAN1.</td>
</tr>
</tbody>
</table>

Manage Your Network

47
The Show Statistics screen displays the following statistics:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN, LAN, or WLAN</td>
<td>The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN)</td>
</tr>
<tr>
<td>Status</td>
<td>The link status of the port.</td>
</tr>
<tr>
<td>TxPkts</td>
<td>The number of packets transmitted on this port since reset or manual clear.</td>
</tr>
<tr>
<td>RxPkts</td>
<td>The number of packets received on this port since reset or manual clear.</td>
</tr>
<tr>
<td>Collisions</td>
<td>The number of collisions received by this port since reset or manual clear.</td>
</tr>
<tr>
<td>Tx B/s</td>
<td>The current line utilization—percentage of current bandwidth used on this port.</td>
</tr>
<tr>
<td>Rx B/s</td>
<td>The average line utilization for this port.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The time elapsed since the last power cycle or reset.</td>
</tr>
<tr>
<td>ADSL Link Downstream or Upstream</td>
<td>The statistics for the upstream and downstream ADSL link. These statistics will be of interest to your technical support representative if you are having problems obtaining or maintaining a connection.</td>
</tr>
<tr>
<td>Connection Speed</td>
<td>Typically, the downstream speed is faster than the upstream speed.</td>
</tr>
<tr>
<td>Line Attenuation</td>
<td>The line attenuation increases the further you are physically located from your ISP’s facilities.</td>
</tr>
<tr>
<td>WAN, LAN, or WLAN</td>
<td>The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:</td>
</tr>
<tr>
<td>Status</td>
<td>The link status of the port.</td>
</tr>
</tbody>
</table>
Connection Status

On the Router Status screen, click the **Connection Status** button to display wireless modem router connection status.

This screen shows the following statistics:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Time</td>
<td>The time elapsed since the last connection to the Internet through the ADSL port.</td>
</tr>
<tr>
<td>Connecting to sender</td>
<td>The connection status.</td>
</tr>
<tr>
<td>Negotiation</td>
<td>Success or Failed.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Success or Failed.</td>
</tr>
<tr>
<td>Obtaining IP Address</td>
<td>The IP address assigned to the WAN port by the ADSL Internet Service Provider.</td>
</tr>
<tr>
<td>Obtaining Network Mask</td>
<td>The network mask assigned to the WAN port by the ADSL Internet Service Provider.</td>
</tr>
</tbody>
</table>
Attached Devices

The Attached Devices screen contains a table of all IP devices that the wireless modem router has discovered on the local network.

Select Maintenance > Attached Devices to view the following screen.

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

Diagnostics and Rebooting

Select Maintenance > Diagnostics to display the following screen.

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

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

Remote management lets you enable a user or users on the Internet to configure, upgrade, and check the status of your wireless modem router.

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

➢ To configure remote management:

1. Select **Advanced > Remote Management**.

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

3. Specify the external addresses allowed to access the router remotely. For security, restrict access to as few as practical:
   - To allow access from any IP address on the Internet, select **Everyone**.
   - To allow access from a range of IP addresses, select **IP address Range**. Then enter a beginning and ending IP address to define the allowed range.
   - To allow access from a single IP address on the Internet, select **Only this Computer**. Enter the IP address that will be allowed access.

4. Specify the port number that will be used for accessing the router menu.
Web browser access usually uses the standard HTTP service port 80. For greater security, you can specify 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 have your changes take effect.

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

**http://134.177.0.123:8080**

In this case, the http:// must be included in the address.
This chapter describes how to configure the advanced features of your wireless modem router. For information about remote management, see *Remote Management* on page 51. The following features are discussed in this chapter:

- **WAN Settings**
- **Default DMZ Server**
- **Dynamic DNS**
- **LAN Settings**
- **Quality of Service (QoS)**
- **Advanced Wireless Settings**
- **Static Routes**
- **Universal Plug and Play**
- **TR069 Client Configuration**
- **Wireless Bridging and Repeating Networks**
WAN Settings

➢ To configure WAN settings:

Select Advanced > WAN Setup to display the following screen.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable PPPoE Relay</td>
<td>When enabled, this feature will allow a PPPoE client on a local PC to connect to a remote PPPoE server with the gateway acting as a relay agent.</td>
</tr>
<tr>
<td>Disable Port Scan and DoS Protection</td>
<td>The SPI (Stateful Packet Inspection) firewall protects your LAN against denial of service attacks. This should only be disabled in special circumstances.</td>
</tr>
<tr>
<td>Default DMZ Server</td>
<td>See Default DMZ Server on page 55.</td>
</tr>
<tr>
<td>Respond to a Ping on an Internet WAN Port</td>
<td>If you want the wireless modem router to respond to a ping from the Internet, select the Respond to Ping on Internet Port check box. This should be used only as a diagnostic tool, since it allows your wireless modem router to be discovered. Do not select this check box unless you have a specific reason to do so.</td>
</tr>
<tr>
<td>MTU Size</td>
<td>The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.</td>
</tr>
<tr>
<td>Disabling the SIP ALG</td>
<td>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.</td>
</tr>
</tbody>
</table>
Default DMZ Server

The default demilitarized zone (DMZ) server feature is helpful when you use some online games and video conferencing applications that are incompatible with NAT. The wireless 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, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is usually discarded by the wireless 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. Select **Advanced > WAN Setup**.

![WAN Setup](image)

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

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

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

➢ To configure 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. The Dynamic DNS service provider might call this the domain name. If your URL is myName.dyndns.org, then 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 configuration.

---

**Note:** If your ISP assigns a private WAN IP address such as 10.0.x.x or 10.x.x.x, the Dynamic DNS service will not work because private addresses will not be routed on the Internet.

---

**LAN Settings**

The LAN Setup screen allows configuration of LAN IP services such as DHCP.

---

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

---

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

- **LAN IP address.** 10.0.0.2
- **Subnet mask.** 255.255.255.0

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

Select Advanced > LAN IP Setup.

DHCP

By default, the wireless modem router functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the wireless modem router’s LAN. The assigned default gateway address is the LAN address of the 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 router are satisfactory.

Use Router as DHCP Server

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

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router’s
LAN IP address. Using the default addressing scheme, you should define a range between 10.0.0.3 and 10.0.0.255, although you might want to save part of the range for devices with fixed addresses.

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

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

Reserved IP Addresses

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

➢ To reserve an IP address:

1. In the LAN Setup screen, click the Add button.

   ![Address Reservation Table]

2. In the IP Address field, type the IP address to assign to the computer or server. Choose an IP address from the router’s LAN subnet, such as 10.0.0.x.

3. Type the MAC address of the computer or server.

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

4. Click Apply to enter the reserved address into the table.
Advanced Configuration

N300 Wireless ADSL2+ Modem Router DGN2200Mv2

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

- **To edit or delete a reserved address entry:**
  1. Click the button next to the reserved address 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 must be 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.

- **To configure QoS for Internet access**
  To specify prioritization of traffic, you must add or create a policy for the type of traffic.
  1. Select **Advanced > QoS Setup**.
2. Click **Setup QoS rule** to display the QoS Priority Rule list:

![QoS Priority Rule list](image)

3. To change a rule, select its radio button.
4. Scroll down to the bottom of the screen:

![QoS Priority Rule list with options](image)

5. To edit a rule, click **Edit**. To add a custom rule, click **Add Priority Rule**.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, click **Apply**.
Advanced Wireless Settings

The advanced WPS settings cannot be displayed if you have selected WEP as the security option.

➢ To display and specify advanced WPS settings:

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

By default the **WPS (Push 'N' Connect) check box** is selected. If you clear this check box and click **Apply**, you will not be able to use WPS.

2. Under WPS Settings, you can configure the following settings:
   • **Disable Router's PIN.** Only when the wireless modem router’s PIN is enabled, can you configure the wireless modem router’s wireless settings or add a wireless client through WPS with the wireless modem router’s PIN number. If the wireless modem router detects suspicious attempts to access the network with a PIN, the PIN function might be disabled temporarily. 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 cleared. This allows the modem router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the modem router automatically selects this check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.

   If you configure your wireless router settings and security manually, the **Keep Existing Wireless Settings** check box will also be selected. This will allow you to use WPS (Push 'N' Connect) to connect additional WPS-capable devices to your wireless network using the existing settings.

3. Click **Apply** to save your settings.
Static Routes

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

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 10.0.0.100.
- Your company’s network address is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP to the wireless modem router, and a second static route was created to your local network for all 10.0.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company’s firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 10.0.0.100.

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 should be forwarded to the ISDN router at 10.0.0.100.
- 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.

➢ **To add a static route**

1. Select **Advanced > Static Routes**.
2. Click **Add** to open the Static Routes screen.

3. Enter a route name for this static route in the **Route Name** field. This name is for identification purpose only.

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

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

6. Enter the destination IP address of the final destination.

7. Enter the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.

8. Enter the gateway IP address, which must be a router on the same LAN segment as the router.

9. Enter a number between 2 and 15 as the metric value in the **Metric** field. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.

10. Click **Apply**. 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.

➢ To configure UPnP:

1. Select UPnP to display the following screen:

2. Fill in the settings on the UPnP screen:
   - **Turn UPnP On.** UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If UPnP is disabled, the wireless modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the wireless modem router.
   - **Advertisement Period.** The advertisement period is how often the wireless 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.** The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value a little.
   - **UPnP Portmap Table.** The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the wireless 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 wireless 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.

**TR069 Client Configuration**

The TR-069 WAN management protocol allows auto-configuration, provisioning, collection, and diagnostics to be performed by an Auto-Configuration Server (ACS).

➢ **To input the TR-069 Client settings:**

1. Select **TR069** to display the following screen:

2. Click **Turn WAN Management Protocol On** to enable TR069 Client.

3. Enter the configuration parameters:
   - **Inform Status.** Select whether the DGN2200Mv2 can send data to the Auto-Configuration Server.
   - **Inform Interval.** The DGN2200Mv2 sends the inform data to ACS at the assigned time interval periodically in order to get updated information.
   - **ACS URL.** Input the IP address of the ACS server that the DGN2200Mv2 will connect to.
   - **ACS Username.** Enter the username the DGN2200Mv2 uses to connect to the ACS server.
   - **ACS Password.** Enter the password the DGN2200Mv2 uses to connect to the ACS server.

4. Click **Apply** when done.
Wireless Bridging and Repeating Networks

With the DGN2200Mv2 wireless 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 by using their MAC addresses rather than by specifying IP addresses.

Here are some examples of wireless bridged configurations:

- **Point-to-point bridge.** The wireless modem router communicates with another bridge-mode wireless station. See *Point-to-Point Bridge Configuration* on page 68.
- **Multi-point bridge.** The wireless modem router is the “master” for a group of bridge-mode wireless stations. Then all traffic is sent to this master, rather than to other access points. See *Multi-Point Bridge* on page 69.
- **Repeater with wireless client association.** Sends all traffic to the remote access point. See *Repeater with Wireless Client Association* on page 70.

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

To view or change these configurations, from the main menu, under Advanced, select *Wireless Settings* and select WDS:
Point-to-Point Bridge Configuration

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

Figure 5. Point-to-Point Bridge Mode

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

1. Configure the DGN2200Mv2 wireless modem router (AP 1) on LAN Segment 1 in point-to-point bridge mode.

2. Configure the other access point (AP 2) on LAN Segment 2 in point-to-point bridge mode.
   The DGN2200Mv2 wireless modem router must have AP 2’s MAC address in its Remote MAC Address field, and AP 2 must have the DGN2200Mv2’s MAC address in its Remote MAC Address field.

3. Configure both APs and verify that both APs are using the same SSID, channel, authentication mode, if any, and 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.
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:

- Enter the MAC addresses of the other access points in the fields provided.
- Set the other bridge-mode access points to point-to-point bridge mode, using the MAC address of this DGN2200Mv2 as the remote MAC address.
- Use wireless security to protect this traffic.

To set up the multi-point bridge configuration:

1. Configure the operating mode of the wireless modem routers.
   - Because it is in a central location, configure the DGN2200Mv2 wireless modem router (AP 1) on LAN segment 1 in point-to-multi-point bridge mode, and enter the MAC addresses of AP 2 and AP 3 in the Remote MAC Address 1 and Remote MAC Address 2 fields.
   - Configure the access point (AP 2) on LAN segment 2 in point-to-point bridge mode with the remote MAC address of the DGN2200Mv2 wireless modem router.
   - Configure the access point (AP 3) on LAN segment 3 in point-to-point bridge mode with the remote MAC address of the DGN2200Mv2 wireless modem router.

2. Disable the DHCP server on AP 2 and AP 3. AP 1 will then be the DHCP server.

3. Verify the following for all access points:
• The LAN network configuration of the wireless modem router and other access points are configured to operate in the same LAN network address range as the LAN devices.

• Only one access point, the DGN2200Mv2 wireless modem router in Figure 6, Multi-Point Bridge Mode, is configured in point-to-multi-point bridge mode; all the others are in point-to-point bridge mode.

• All APs, including the DGN2200Mv2 wireless modem router, must be on the same LAN. That is, all the access point LAN IP addresses must be in the same network.

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

• All APs, including the DGN2200Mv2 wireless modem router, must use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.

• All point-to-point APs must have the MAC address of AP 1 (the DGN2200Mv2 wireless modem router in the previous figure) in the **Remote AP MAC address** field.

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

---

**Note:** Wireless stations configured as they are in *Figure 5* on page 68 will not be able to connect to the wireless modem router or access points. If you require wireless stations to access any LAN segment, you can use additional access points configured in wireless access point mode in any LAN segment.

---

**Repeater with Wireless Client Association**

In the repeater mode with wireless client association, the DGN2200Mv2 wireless modem router sends all traffic to a remote access point. For the repeater mode, you must enter the MAC address of the remote “parent” access point. Alternatively, you can configure the DGN2200Mv2 wireless modem router as the parent by entering the address of a “child” access point. Note that the following restrictions apply:

• **You do not** have the option of disabling client associations with this DGN2200Mv2 wireless modem router.

• You cannot configure a sequence of parent-child APs. You are limited to only one parent access point, although if the DGN2200Mv2 wireless modem router is the parent access point, it can connect with up to four child APs.
The following figure shows an example of a repeater mode configuration.

**Figure 7. Repeater Mode**

- **To set up a repeater with wireless client association:**
  1. Configure the operating mode of the devices.
     - Configure AP 1 (the DGN2200Mv2 wireless modem router in *Figure 7, Repeater Mode*) with the MAC address of AP 2 and AP 3 in the first two *Remote MAC Address* fields.
     - Configure AP 2 with the MAC address of AP 1 in the *Remote MAC Address* field.
     - Configure AP 3 with the MAC address of AP 1 in the *Remote MAC Address* field.
  2. Verify the following for both access points:
     - The LAN network configuration of each access point is configured to operate in the same LAN network address range as the LAN devices.
     - The access points must be on the same LAN. That is, the LAN IP addresses for the access points must be in the same network.
     - If you are using DHCP, access point devices should be set to *Obtain an IP address automatically (DHCP Client)* in the IP Address Source section of the Basic IP Settings screen.
     - Access point devices must use the same SSID, channel, authentication mode, and encryption.
  3. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.
VPN Lite is a secure, easy-to-use, and cost-effective virtual private network (VPN). With VPN Lite, you can configure the network that is right for you with the flexibility to adjust the configuration as your business needs change. A VPN Lite configuration consists of sites and individual connections. A site is a device within your VPN network that is identified by a private static IP address. Each site within the network has a private VPN connection with any other site in the network. You can connect up to 50 sites on a VPN Lite network without affecting your monthly ADSL ISP bill.

**Note:** To learn more about the Telkom VPN Lite service offering, log in to the Telkom VPN Lite web portal at [http://www.telkom.co.za/products_services/vpn/vpnlite/index.html](http://www.telkom.co.za/products_services/vpn/vpnlite/index.html).
Configuring VPN Lite Sites

The VPN Lite Setup Wizard lets you configure your VPN Lite network connections one-by-one.

➢ To use the VPN Lite Wizard:

1. Log in to your router as described in Log In on page 7.
2. Select VPN Lite Wizard to display the following screen:

   ![Figure 8. Select VPN Lite Wizard](image)

3. Read the notice on the VPN Lite setup screen and click Next to continue.
4. Enter the information for one of the sites that you configured on the Telkom VPN Lite web portal and click Next.

   ![Figure 9. Enter user name and password](image)

For the site that you are adding to your network:

**Username.** Enter the user name that you configured.

**Password.** Enter the password that you configured.

**LAN IP/netmask.** Enter the private and static IP address that you configured.

---

**Note:** The IP address for each site configured must be different and fall within a different IP Subnet range. Example: site1@evpn.lite.0001 can be 10.0.1.0/24, then the IP subnet for site2@evpn.lite.0002 must be a different subnet, like 10.0.2.0/24. The IP Address must correspond exactly to the one configured on the VPN Lite Webpage.
5. Review the configuration details and click **Finish** to complete the VPN Lite setup:

![VPN Lite Site Confirmation](image)

*Note:* After selecting Finish, you might need to connect to your router with the new LAN IP address entered when you configured VPN Lite. Please wait until the progress bar on the router menu page has completed before attempting to reconnect.

6. Repeat Steps 1 through 4 for every VPN Lite site you want to add to your network.
This chapter provides information about troubleshooting your N300 Wireless ADSL2+ Modem Router DGN2200Mv2. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- **Is the router on?**
  Go to *Basic Functioning* on page 76.

- **Have I connected the router correctly?**
  Go to *Basic Functioning* on page 76.

- **I cannot access the router’s configuration with my browser.**
  Go to *Cannot Log In to the Wireless Modem Router* on page 78.

- **I have configured the router but I cannot access the Internet.**
  Go to *Troubleshooting the Internet Connection* on page 78.

- **I cannot remember the router’s configuration password.**
  Go to *Restoring the Default Configuration and Password* on page 83.

- **I want to clear the configuration and start over again.**
  Go to *Restoring the Default Configuration and Password* on page 83.
Basic Functioning

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

1. When power is first applied, verify that the Power LED is on.
2. After approximately 10 seconds, verify the following:
   • The LAN port LEDs are lit for any local ports that are connected.
   • The ADSL Link LED is lit.

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

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

Welcome Screen Displays instead of Router Main Menu

This situation can occur if the CD Setup Wizard does not complete successfully; the unit stays in Wizard Mode. If the Welcome screen displays instead of the main menu when you try to go to the Internet or log into the wireless modem router, you can bypass the wizard using one of the following methods:

• Log in to the wireless modem router at http://routerlogin.com/basicsetting.htm.
• Reset the wireless modem router to factory defaults to take the router out of Wizard Mode altogether.

Troubleshooting with the LEDs

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

1. When power is first applied, verify that the Power LED is on.
2. After approximately 10 seconds, verify that:
   • The Power LED is green.
   • The LAN port LEDs are lit for any local ports that are connected. If a LAN port is connected to a 100 Mbps device, verify that the port’s LED is green. If the port is 10 Mbps, the LED is amber.
   • The ADSL link LED is lit, indicating that a link has been established to the connected device.
   • The Wireless LEDs are lit.
If any of the above conditions does not occur, see the following table.

<table>
<thead>
<tr>
<th>Situation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power LED is off.</td>
<td>If the Power and other LEDs are off when your router is turned on: \n• Make sure the power cord is securely connected to your router and that the power supply adapter is securely connected to a functioning power outlet. \n• Check that you are using the power adapter supplied by NETGEAR for this product. \nIf the error persists, you have a hardware problem and should contact Technical Support.</td>
</tr>
<tr>
<td>Power LED is red.</td>
<td>If the Power LED remains red, there is a fault within the router. \n• Cycle the power to see if the router recovers. \n• Clear the router’s configuration to factory defaults. This sets the router’s IP address to 10.0.0.2. This procedure is explained in <em>Restoring the Default Configuration and Password</em> on page 83. \nIf the error persists, you might have a hardware problem and should contact Technical Support.</td>
</tr>
<tr>
<td>LEDs never turn off.</td>
<td>When the router is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the router. \nIf all LEDs are still on 1 minute after power-up: \n• Cycle the power to see if the router recovers. \n• Clear the router’s configuration to factory defaults as explained in <em>Restoring the Default Configuration and Password</em> on page 83. \nIf the error persists, you might have a hardware problem and should contact Technical Support at <a href="http://www.netgear.com/support">www.netgear.com/support</a>.</td>
</tr>
<tr>
<td>ADSL Link LED is off.</td>
<td>• Disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones. \n• Check that the telephone company has made the connection to your line and tested it. \n• 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 of the RJ-11 jack. The N300 Modem Router uses pins 2 and 3.</td>
</tr>
<tr>
<td>Internet LED is red.</td>
<td>The wireless modem router cannot access the Internet. See <em>Internet LED Is Red</em> on page 79.</td>
</tr>
<tr>
<td>The Ethernet port LEDs are off.</td>
<td>If the Ethernet port LEDs do not light when the Ethernet connection is made, check the following: \n• Make sure that the Ethernet cable connections are secure at the wireless modem router and computer. \n• Make sure that power is turned on to the connected modem or computer.</td>
</tr>
<tr>
<td>Wireless LEDs are off.</td>
<td>If the Wireless LEDs do not come on, verify that the <strong>Enable Wireless Router Radio</strong> check box is selected on the Wireless Settings screen. See <em>Manually Configure Wireless Settings</em> on page 22.</td>
</tr>
</tbody>
</table>
Cannot Log In to the Wireless Modem Router

If you are unable to log in to the wireless 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 router as described in the previous section.
- Make sure that your computer’s IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer’s address should be in the range of 10.0.0.3 to 10.0.0.255.
- If your computer’s IP address is shown as 169.254.x.x, recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.
- If your router’s IP address was changed and you do not know the current IP address, clear the router’s configuration to factory defaults. This sets the router’s IP address to 10.0.0.2. This procedure is explained in Using the Restore Factory Settings Button to Reset the Router on page 83.
- 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 admin. Make sure that Caps Lock is off when you enter this information.

If the router does not save changes you have made while logged in, check the following:

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

Troubleshooting the Internet Connection

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

ADSL Link

If your router is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the Internet LED.
N300 Wireless ADSL2+ Modem Router DGN2200Mv2

**ADSL Link LED Is Green or Blinking Green**

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

**ADSL Link LED Is Blinking Amber**

If your ADSL link LED is blinking amber, then your wireless 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 wireless 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 the router that cannot connect to the Internet but your ISP that cannot provide an Internet connection.
Obtaining an Internet IP Address

If your wireless modem router is unable to access the Internet, and your Internet LED is green or blinking green, you should determine whether the wireless modem router is able to obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your wireless modem router must request an IP address from the ISP. You can determine whether the request was successful 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 wireless modem router’s configuration at http://10.0.0.2.
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 wireless modem router has not obtained an IP address from your ISP.

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

• 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 wireless 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 router’s MAC address.
  - Configure your router to spoof your computer’s MAC address. This can be done in the Basic Settings screen.

Troubleshooting PPPoE or PPPoA

The PPPoE or PPPoA connection can be debugged as follows:

1. Access the main menu of the router at http://10.0.0.2.
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 wireless 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.
Troubleshooting Internet Browsing

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

• Your computer might not recognize any DNS server addresses.

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

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

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

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer.

Testing the LAN Path to Your Wireless Modem Router

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

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

1. From the Windows toolbar, click the Start button, and select Run.
2. In the field provided, type ping followed by the IP address of the router, as in this example: ping 10.0.0.2
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 *Troubleshooting with the LEDs* on page 76.
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.

- **Wrong network configuration**
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

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

After verifying that the LAN path works correctly, test the path from your PC to a remote device. 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 in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default wireless modem router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC’s Network Control Panel. Verify that the IP address of the router is listed as the default wireless modem router.

- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

- Check that your cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to “clone” or “spoof” the MAC address from the authorized PC.
Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router’s administration password to **admin** and the IP address to **10.0.0.2**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function (see Back Up, Restore, and Erase Your Settings on page 44).
- Press the Restore Factory Settings button on the bottom of the router.

Using the Restore Factory Settings Button to Reset the Router

To restore the factory default configuration settings when you do not know the administration password or IP address, use the Restore Factory Settings button on the bottom of the router:

1. Press and hold the Restore button until the Power LED turns red (about 6 seconds).
2. Release the Restore button. The LED blinks red three times and then turns green when the router has reset to the factory default state. Wait for the router to reboot.

Problems with Date and Time

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

- **Date shown is January 1, 2000.**
  Cause. The router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.

- **Time is off by one hour.**
  Cause. The router does not automatically sense daylight savings time. In the Schedule screen, select the **Adjust for Daylight Savings Time** check box.
This appendix includes technical specifications for the N300 Wireless ADSL2+ Modem Router DGN2200Mv2.

- Technical Specifications
- Telkom Factory Default Configuration
## Technical Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network protocol and standards compatibility</td>
<td>TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM</td>
</tr>
</tbody>
</table>
| 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  
WAN: ADSL, Dual RJ-11, pins 2 and 3  
T1.413, G.DMT, G.Lite  
ITU Annex A or B  
ITU G.992.5 (ADSL2+) |
Telkom Factory Default Configuration

You can use the Restore Factory Settings button on the bottom panel of your router to restore factory default settings. Press this button for 6 seconds. Your router will return to the factory configuration settings shown in the following table.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Router Login</strong></td>
<td></td>
</tr>
<tr>
<td>User login URL</td>
<td><a href="http://www.routerlogin.com">http://www.routerlogin.com</a></td>
</tr>
<tr>
<td>User name (case-sensitive)</td>
<td>admin</td>
</tr>
<tr>
<td>Login password (case-sensitive)</td>
<td>admin</td>
</tr>
<tr>
<td><strong>Internet connection</strong></td>
<td></td>
</tr>
<tr>
<td>WAN MAC address</td>
<td>Use default address</td>
</tr>
<tr>
<td>WAN MTU size</td>
<td>1492</td>
</tr>
<tr>
<td>Port speed</td>
<td>Autosensing</td>
</tr>
<tr>
<td><strong>Local network (LAN)</strong></td>
<td></td>
</tr>
<tr>
<td>LAN IP</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DHCP server</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>Local network (LAN) continued</strong></td>
<td></td>
</tr>
<tr>
<td>DHCP starting IP address</td>
<td>10.0.0.3</td>
</tr>
<tr>
<td>DHCP ending IP address</td>
<td>10.0.0.254</td>
</tr>
<tr>
<td>DMZ</td>
<td>Enabled or disabled</td>
</tr>
<tr>
<td>Time zone</td>
<td>GMT + 2:00</td>
</tr>
<tr>
<td>Time zone adjusted for daylight savings time</td>
<td>Automatic</td>
</tr>
<tr>
<td>SNMP</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td></td>
</tr>
<tr>
<td>Inbound (communications coming in from the Internet)</td>
<td>Disabled (except traffic on port 80, the HTTP port)</td>
</tr>
<tr>
<td>Outbound (communications going out to the Internet)</td>
<td>Enabled (all)</td>
</tr>
<tr>
<td>Source MAC filtering</td>
<td>Disabled</td>
</tr>
<tr>
<td>Feature</td>
<td>Default Behavior</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wireless</td>
<td>Wireless communication Enabled</td>
</tr>
<tr>
<td>SSID name</td>
<td>Printed on bottom label. Generated by LAN MAC address.</td>
</tr>
<tr>
<td>Security</td>
<td>WPA-PSK + WPA2-PSK</td>
</tr>
<tr>
<td>Broadcast SSID</td>
<td>Enabled</td>
</tr>
<tr>
<td>Country/region</td>
<td>Europe</td>
</tr>
<tr>
<td>RF channel</td>
<td>Selected based on LAN MAC address</td>
</tr>
<tr>
<td>Operating mode</td>
<td>Up to 145 Mbps</td>
</tr>
<tr>
<td>Data rate</td>
<td>Best</td>
</tr>
<tr>
<td>Output power</td>
<td>Full</td>
</tr>
<tr>
<td>Access point</td>
<td>Enabled</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Open System</td>
</tr>
<tr>
<td>Wireless card access list</td>
<td>All wireless stations allowed</td>
</tr>
</tbody>
</table>
Notification of Compliance

NETGEAR Wireless Routers, Gateways, APs

Regulatory Compliance Information

Note: 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.

Europe – EU Declaration of Conformity

Marking by 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 (2.4Ghz), EN301 489-17 EN60950-1

For complete DoC, visit the NETGEAR EU Declarations of Conformity website at:
http://support.netgear.com/app/answers/detail/a_id/11621/

EDOC in Languages of the European Community

<table>
<thead>
<tr>
<th>Language</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cesky [Czech]</td>
<td>NETGEAR Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími příslušnými ustanoveními směrnic 1999/5/ES.</td>
</tr>
<tr>
<td>Dansk [Danish]</td>
<td>Undertegnede NETGEAR Inc. erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.</td>
</tr>
<tr>
<td>English</td>
<td>Hereby, NETGEAR Inc., declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.</td>
</tr>
<tr>
<td>Language</td>
<td>Text</td>
</tr>
<tr>
<td>-----------</td>
<td>------</td>
</tr>
<tr>
<td>Español [Spanish]</td>
<td>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.</td>
</tr>
<tr>
<td>Ελληνική [Greek]</td>
<td>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR Inc. ΔΗΛΩΝΕΙ ΌΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.</td>
</tr>
<tr>
<td>Français [French]</td>
<td>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.</td>
</tr>
<tr>
<td>Italiano [Italian]</td>
<td>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.</td>
</tr>
<tr>
<td>Nederlands [Dutch]</td>
<td>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.</td>
</tr>
<tr>
<td>Magyar [Hungarian]</td>
<td>Alulírott, NETGEAR Inc. nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.</td>
</tr>
<tr>
<td>Polski [Polish]</td>
<td>Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.</td>
</tr>
<tr>
<td>Português [Portuguese]</td>
<td>NETGEAR Inc. declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.</td>
</tr>
<tr>
<td>Slovensko [Slovak]</td>
<td>NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.</td>
</tr>
<tr>
<td>Slovensky [Slovak]</td>
<td>NETGEAR Inc. týmto vyhlasuje, že Radiolan splňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.</td>
</tr>
<tr>
<td>Svenska [Swedish]</td>
<td>Härem intygar NETGEAR Inc. att denna Radiolan står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.</td>
</tr>
</tbody>
</table>
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.

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, San Jose, CA 95134, declare under our sole responsibility that the N300 Wireless ADSL2+ Modem Router DGN2200Mv2 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 (TBD) 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.

**Industry Canada**

This device complies with RSS-210 of the Industry Canada 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.

**IMPORTANT NOTE: Radiation Exposure Statement:**

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

**Caution:**

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

**NOTE IMPORTANTE: Déclaration d'exposition aux radiations:**

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

**GPL License Agreement**

GPL may be included in this product; to view the GPL license agreement go to [ftp://downloads.netgear.com/files/GPLnotice.pdf](ftp://downloads.netgear.com/files/GPLnotice.pdf).

For GNU General Public License (GPL) related information, please visit [http://support.netgear.com/app/answers/detail/a_id/2649](http://support.netgear.com/app/answers/detail/a_id/2649).
# Interference Reduction Table

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

<table>
<thead>
<tr>
<th>Household Appliance</th>
<th>Recommended Minimum Distance (in feet and meters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microwave ovens</td>
<td>30 feet / 9 meters</td>
</tr>
<tr>
<td>Baby Monitor - Analog</td>
<td>20 feet / 6 meters</td>
</tr>
<tr>
<td>Baby Monitor - Digital</td>
<td>40 feet / 12 meters</td>
</tr>
<tr>
<td>Cordless phone - Analog</td>
<td>20 feet / 6 meters</td>
</tr>
<tr>
<td>Cordless phone - Digital</td>
<td>30 feet / 9 meters</td>
</tr>
<tr>
<td>Bluetooth devices</td>
<td>20 feet / 6 meters</td>
</tr>
<tr>
<td>ZigBee</td>
<td>20 feet / 6 meters</td>
</tr>
</tbody>
</table>
Index

Numerics
3G Mobile Broadband Settings 8

A
access
   restricting 25
   router password 33
access lists 25
address reservation 58
admin user name 33
ADSL settings 16
Advanced Wireless Settings screen 62
antenna, position 20
attached devices, viewing 50

B
backup configuration file 44
Basic Settings screen 13
blocking
   keywords 34
   services 35
   sites 34
bridged networks 67

C
client, WPS 29, 30
compliance 88
configuration file 44
Connection Status screen 49

D
date and time 83
daylight savings time 38, 83
default DMZ server 55
denial of service (DoS) protection 34
DHCP 58
diagnostics 50
DMZ server 55
DNS server 9, 10
   primary 15
   secondary 15
   secondary DNS server 10
Dynamic DNS 56

E
e-mail notification of security events 40
Ethernet LED, troubleshooting and 77

F
factory settings, restoring 44
filtering 25
firewall services, scheduling 37, 38

H
host name 15

I
Internet connection
   troubleshooting 78, 79, 81
Internet LED, troubleshooting 77
IP address 7, 14, 15
   attached device 50
   DMZ server 55
   dynamic 56
   factory default 44
   LAN settings 58
   PPPoE 49
   remote management 51
   Router Status screen 46
   static 10
IP address reservation 59
IP subnet mask 58
ISP settings 13

K
keywords, blocking 34

L
LAN settings 57, 58
location, router 20
logging in 7, 33
logging out 7
login time-out 34
logs 39, 40

M
MAC address
filtering 25
rejected 82
restricting access by 25
spoofing 80
metric (static routes) 64
Mobile Broadband Settings 12
MTU size 54
multi-point bridge mode 69

N
Network Time Protocol 37, 83
networks
adding clients 29, 30

P
password 7, 33
PIN, WPS 30
ping 54, 81, 82
placing router 20
plug and play 65
point-to-point bridge mode 68
Power LED, troubleshooting 76
PPPoA or PPPoE
   troubleshooting 80
preset security 19
primary DNS server 9, 10, 15
Push 'N' Connect 28

Q
Quality of Service (QoS) 60

R
range, wireless connections 20
rebooting from the Diagnostics screen 50
remote management 51
repeater mode with wireless client association 70
reserved IP addresses 59
restoring
   configuration file 44
   factory settings 44
router location 20
router statistics 47
router status 45

S
scheduling firewall services 37, 38
secondary DNS server 9
sending logs by email 40
services, blocking 35
Setup Wizard 8
SIP ALG 54
SMTP 41
SPI firewall 54
spoofing 25
static IP address 10
static routes 63
statistics, router 47
status, connection 49
syslog 39

T
TCP/IP network troubleshooting 81
technical support 2
time 37, 83
time zone 38
timeout, administrator login 34
time-stamping 38
trademarks 2
troubleshooting
   general information 75
   Internet browsing 81
   Internet connection 78, 79
   LEDs 76, 77, 79
   log in access 78
   network 81
   PPPoA or PPPoE 80
time 83
trusted host 35

U
Universal Plug and Play (UPnP) 65
usage statistics 45
user name 7

V
VPN Lite 72
VPN Lite Wizard 73

W

WAN settings 54
  MTU size 54
  ping 54
  SIP ALG 54
  SPI Firewall 54
WEP 26
Wi-Fi Protected Setup (WPS) 28, 62
WINS 59
wireless bridging and repeating 67
wireless distribution system (WDS) 67, 68, 69, 70
Wireless LED, troubleshooting 77
wireless mode 23
wireless network, range and interference 20
wireless security 20
Wireless settings 22
wireless settings 22
  advanced 62
WLAN 48
WLAN statistics 48
WPA 26
WPA+WPA2 26
WPA2 26
WPS 28
WPS button 28
WPS PIN 30