

Wireless-N 300 Modem Router DGN2200 User Manual



NETGEAR®

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134 USA

208-10563-01
November 2009
v1.0

Trademarks

NETGEAR, the NETGEAR logo, and RangeMax are trademarks or registered trademarks of NETGEAR, Inc. in the United States and/or other countries. Microsoft, Windows, and Windows NT are registered trademarks and Vista is a trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders.

Statement of Conditions

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

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

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

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

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

Federal Communications Commission (FCC) Radiation Exposure Statement

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

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.

European Union Statement of Compliance

Hereby, NETGEAR, Inc. declares that this wireless-N modem router is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Česky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento Wireless-N 300 Modem Router DGN2200 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr Wireless-N 300 Modem Router DGN2200 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät Wireless-N 300 Modem Router DGN2200 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme Wireless-N 300 Modem Router DGN2200 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this Wireless-N 300 Modem Router DGN2200 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente NETGEAR, Inc. declara que el Wireless-N 300 Modem Router DGN2200 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR, Inc. ΔΗΛΩΝΕΙ ΟΤΙ Wireless-N 300 Modem Router DGN2200 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente NETGEAR, Inc. déclare que l'appareil Wireless-N 300 Modem Router DGN2200 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente NETGEAR, Inc. dichiara che questo Wireless-N 300 Modem Router DGN2200 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarē, ka Wireless-N 300 Modem Router DGN2200 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis Wireless-N 300 Modem Router DGN2200 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel Wireless-N 300 Modem Router DGN2200 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, NETGEAR, Inc., jiddikjara li dan Wireless-N 300 Modem Router DGN2200 jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a Wireless-N 300 Modem Router DGN2200 megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oświadczam, że Wireless-N 300 Modem Router DGN2200 jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este Wireless-N 300 Modem Router DGN2200 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta Wireless-N 300 Modem Router DGN2200 v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že Wireless-N 300 Modem Router DGN2200 spáda základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että Wireless-N 300 Modem Router DGN2200 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna [utrustningstyp] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the DGN2200 product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Wireless-N 300 Modem Router DGN2200 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the Wireless-N 300 Modem Router DGN2200 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your Wireless-N 300 Modem Router DGN2200.

World Wide Web

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

Product and Publication Details

Model Number:	DGN2200
Publication Date:	November 2009
Product Family:	Wireless-N Modem Router
Product Name:	Wireless-N 300 Modem Router DGN2200
Home or Business Product:	Home
Language:	English
Publication Part Number:	208-10563-01
Publication Version Number:	1.0

Contents

Wireless-N 300 Modem Router DGN2200 User Manual

About This Manual

Conventions, Formats, and Scope	xi
Revision History	xii

Chapter 1

Configuring Your Internet Connection

Using the Setup Manual	1-1
Logging In to Your Wireless-N Modem Router	1-2
Using the Setup Wizard	1-4
Viewing or Manually Configuring Your ISP Settings	1-5
Configuring ADSL Settings	1-9

Chapter 2

Configuring Your Wireless Network and Security Settings

Planning Your Wireless Network	2-1
Wireless Placement and Range Guidelines	2-2
Wireless Security Options	2-3
Manually Configuring Your Wireless Network	2-4
Manually Configuring Your Wireless Security	2-8
Configuring WPA-PSK (TKIP) + WPA2-PSK (AES) Security	2-8
Configuring WEP	2-9
Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security	2-11
Connecting Additional Wireless Client Devices After WPS Setup	2-14
Wireless Guest Networks	2-15

Chapter 3

Protecting Your Network

Protecting Access to Your Wireless-N Modem Router	3-1
Changing the Built-In Password	3-2
Changing the Administrator Login Time-out	3-3

Blocking Keywords, Sites, and Services	3-3
Blocking Sites	3-3
Blocking Services	3-5
Setting Times and Scheduling Firewall Services	3-7
Setting Your Time Zone	3-7
Scheduling Firewall Services	3-8
Viewing, Selecting, and Saving Logged Information	3-9
Examples of Log Messages	3-10
Enabling Security Event E-mail Notification	3-11

Chapter 4

Managing Your Network

Upgrading the Firmware	4-1
Manually Checking for Firmware Upgrades	4-2
Automatic Firmware Recovery	4-3
Backing Up, Restoring, and Erasing Your Settings	4-4
Backing Up the Configuration to a File	4-4
Restoring the Configuration from a File	4-5
Erasing the Configuration	4-5
Network Management Information	4-6
Router Status and Usage Statistics	4-6
Viewing Attached Devices	4-11
Running Diagnostic Utilities and Rebooting the Wireless-N Modem Router	4-11
Configuring Remote Management	4-12

Chapter 5

USB Storage

USB Drive Requirements	5-2
File Sharing Scenarios	5-2
Sharing Photos with Friends and Family	5-3
Sharing Large Files with Colleagues	5-3
USB Storage Basic Settings	5-4
Editing a Network Folder	5-6
Configuring USB Storage Advanced Settings	5-7
Creating a Network Folder	5-9
Unmounting a USB Drive	5-9
Specifying Approved USB Devices	5-10

Connecting to the USB Drive from a Remote Computer	5-11
Locating the Internet Port IP Address	5-11
Accessing the Router's USB Drive Remotely Using FTP	5-11
Connecting to the USB Drive with Microsoft Network Settings	5-11

Chapter 6

Advanced Configuration

Configuring WAN Settings	6-1
Setting Up a Default DMZ Server	6-3
Configuring Dynamic DNS	6-4
Configuring LAN Settings	6-6
Configuring DHCP	6-7
Configuring Reserved IP Addresses	6-8
Setting up Quality of Service (QoS)	6-9
Configuring QoS for Internet Access	6-9
Advanced Wireless Settings	6-11
Restricting Wireless Access to Your Network	6-11
Configuring WPS Settings	6-14
Using Static Routes	6-15
Static Route Example	6-15
Configuring Static Routes	6-16
Configuring Universal Plug and Play	6-18
Building Wireless Bridging and Repeating Networks	6-19
Point-to-Point Bridge Configuration	6-21
Multi-Point Bridge	6-22
Repeater with Wireless Client Association	6-24
Port Forwarding and Port Triggering	6-25
Port Forwarding	6-25
Port Triggering	6-26
Advanced USB Settings	6-27
Traffic Meter	6-28

Chapter 7

Troubleshooting

Basic Functioning	7-1
Welcome Page Displays instead of Router Main Menu	7-2
Power LED Is Off	7-2

Power LED Is Red	7-2
LAN or ADSL Port LED Is Off	7-3
Window Appears Asking You to Reload Firmware	7-3
Cannot Log in to the Wireless-N Modem Router	7-3
Troubleshooting the ISP Connection	7-4
ADSL Link	7-4
Internet LED is Red	7-5
Obtaining an Internet IP Address	7-6
Troubleshooting PPPoE or PPPoA	7-6
Troubleshooting Internet Browsing	7-7
Resolving a 'Reload Firmware' Message	7-7
Troubleshooting a TCP/IP Network Using the Ping Utility	7-8
Testing the LAN Path to Your Wireless-N Modem Router	7-8
Testing the Path from Your Computer to a Remote Device	7-9
Restoring the Default Configuration and Password	7-10
Using the Wireless On/Off and WPS Buttons to Reset the Router	7-10
Problems with Date and Time	7-10

Appendix A

Wall Mounting and Technical Specifications

Wall-Mounting Your Modem Router	A-1
General Specifications	A-3
Factory Default Configuration	A-4

Appendix B

Related Documents

Index

About This Manual

The *NETGEAR® Wireless-N ADSL2+ Modem Router DGN2200 User Manual* describes how to install, configure and troubleshoot the Wireless-N 300 Modem Router DGN2200. The information in this manual is intended for readers with intermediate computer and Internet skills.


Conventions, Formats, and Scope


The conventions, formats, and scope of this manual are described in the following paragraphs:


- **Typographical Conventions.** This manual uses the following typographical conventions::

<i>Italic</i>	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
Fixed	Command prompt, CLI text, code
<i>italic</i>	URL links

- **Formats.** This manual uses the following formats to highlight special messages:

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

	Tip: This format is used to highlight a procedure that will save time or resources.
---	--

	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.
---	--

- **Scope.** This manual is written for the Modem Router according to these specifications:

Product Version	Wireless-N 300 Modem Router DGN2200
Manual Publication Date	November 2009

For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in [Appendix B, “Related Documents.”](#)



Note: Product updates are available on the NETGEAR, Inc. website at <http://kbserver.netgear.com/products/DGN2200.asp>.

Revision History

Part Number	Version Number	Date	Description
202-10563-01	1.0	October 2009	Original publication

Chapter 1

Configuring Your Internet Connection

This chapter describes how to configure your Modem Router Internet connection. When you install your wireless-N modem router using the *Resource CD* as described in the *Setup Manual*, these settings are configured automatically for you. This chapter provides instructions on how to log in to the wireless-N modem router for further configuration.



Note: NETGEAR recommends that Windows OS users use the Smart Wizard™ on the *Resource CD* for initial configuration. Mac and Linux OS users should access the *Setup Manual* on the *Resource CD*.

This chapter includes:

- “Using the Setup Manual”
- “Logging In to Your Wireless-N Modem Router” on page 1-2
- “Using the Setup Wizard” on page 1-4
- “Viewing or Manually Configuring Your ISP Settings” on page 1-5
- “Configuring ADSL Settings” on page 1-9

Using the Setup Manual

For first-time installation of your wireless wireless-N modem router, refer to the *Setup Manual*. The Setup Manual explains how to launch the NETGEAR Smart Wizard on the *Resource CD* to step you through the procedure to connect your wireless-N modem router and computers. The Smart Wizard will assist you in configuring your wireless settings and enabling wireless security for your network. After initial configuration using the Setup Manual, you can use the information in this Reference Manual to configure additional features of your wireless wireless-N modem router.

For installation instructions in a language other than English, see the language options on the *Resource CD*.

Logging In to Your Wireless-N Modem Router

You can log in to the wireless-N modem router to view or change its settings. Links to Knowledge Base and documentation are also available on the wireless-N modem router main menu.



Note: Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document in [“Preparing Your Network” in Appendix B](#).

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

To log in to the wireless-N modem router:

1. Type **http://www.routerlogin.com**, or the wireless-N modem router’s LAN IP address (default is 192.168.0.1) in the address field of your browser, and then press Enter. A login window displays:



Figure 1-1

2. Enter **admin** for the wireless-N modem router user name and your password (or the default, **password**). For information about how to change the password, see [“Changing the Built-In Password” on page 3-2](#).



Note: The wireless-N 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.

If the wireless-N modem router has never been configured, the Smart Wizard screen displays. After the wireless-N modem router has been configured, the Firmware Upgrade assistant will appear.

- **Checking for Firmware Updates screen.** After initial configuration, this screen displays unless you previously cleared the **Check for Updated Firmware Upon Log-in** check box.

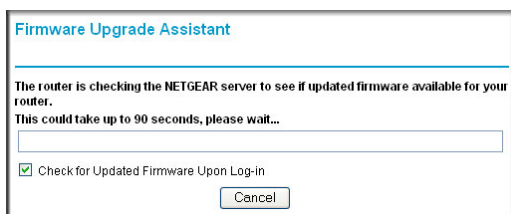
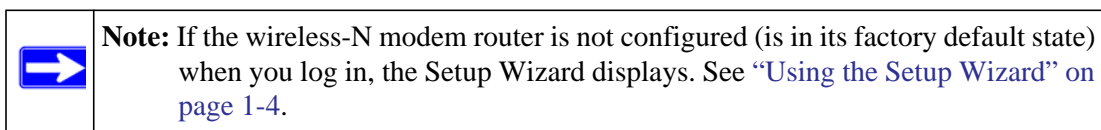


Figure 1-2



If the wireless-N modem router discovers a newer version of the firmware, you are asked if you want to upgrade to the new firmware (see [“Upgrading the Firmware”](#) on page 4-1 for details). If no new firmware is available, the following message displays.

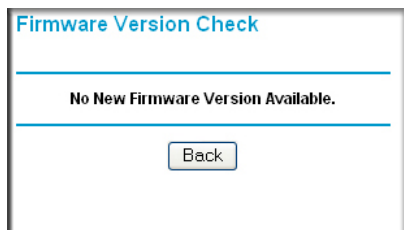


Figure 1-3

- **Router Status screen.** The Router Status screen displays if the wireless-N modem router has not been configured yet or has been reset to its factory default settings. See [“Viewing Modem Router Status Information”](#) on page 4-4.

You can use the Setup Wizard to automatically detect your Internet connection as described in [“Using the Setup Wizard”](#) on page 1-4, or you can bypass the Setup Wizard and manually configure your Internet connection as described in [“Viewing or Manually Configuring Your ISP Settings”](#) on page 1-5.

Using the Setup Wizard

You can manually configure your Internet connection using the Basic Settings screen, or you can allow the Setup Wizard to detect your Internet connection. The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration. This feature is not the same as the Smart Wizard on the *Resource CD* that is used for installation.

To use the Setup Wizard:

1. To go to the Setup Wizard screen, from the top of the main menu, select Setup Wizard.

Figure 1-4

2. Select **Yes** for the Auto-Detect Connection Type, and then click **Next** to proceed.

Enter your ISP settings, as needed. The Setup Wizard detects your ISP configuration.

Depending on the type of connection, you are prompted to enter your ISP settings, as shown in the following table.

Table 1-1. Auto-Detected Internet Connection Types

Connection Type	ISP Information
PPP over Ethernet (PPPoE) PPP over ATM (PPPoA)	Enter the login user name and password. These fields are case-sensitive.
Dynamic IP Account Setup	No entries needed.

Table 1-1. Auto-Detected Internet Connection Types (continued)

Connection Type	ISP Information
IP over ATM Classical IP assignment (RFC1577)	<ul style="list-style-type: none"> • Enter the assigned IP address, subnet mask, and the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. • DNS servers are required to perform the function of translating an Internet name such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here.
Fixed IP (Static) Account Setup	<ol style="list-style-type: none"> 1. If required, enter the account name and domain name from your ISP. 2. 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. 3. Enter your assigned IP address, subnet mask, and the IP address of your ISP's gateway wireless-N modem router. This information should have been provided to you by your ISP. 4. Enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also. <p>DNS servers are required to perform the function of translating an Internet name such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here.</p>

3. At the end of the Setup Wizard, click **Test** to verify your Internet connection. If you have trouble connecting to the Internet, see [Chapter 8, "Troubleshooting."](#)

Viewing or Manually Configuring Your ISP Settings

To view or configure the basic settings:

1. Log in to the wireless-N modem router as described in ["Logging In to Your Wireless-N Modem Router"](#) on page 1-2.

Select Basic Settings from the wireless-N modem router menu to display the Basic Settings screen. The fields that are displayed depend on whether or not your Internet connection requires a login.

ISP does not require login

Basic Settings

Does your Internet connection require a login?
 Yes
 No

Account Name (If Required)
 Domain Name (If Required)

Internet IP Address
 Get Dynamically from ISP
 Use Static IP Address
 IP Address
 IP Subnet Mask
 Gateway IP Address

Use IP Over ATM (IPoA)
 IP Address
 IP Subnet Mask
 Gateway IP Address

Domain Name Server (DNS) Address
 Get Automatically from ISP
 Use These DNS Servers
 Primary DNS
 Secondary DNS

NAT (Network Address Translation)
 Enable Disable

Router MAC Address
 Use Default Address
 Use Computer MAC Address
 Use This MAC Address

ISP does require login

Basic Settings

Does your Internet connection require a login?
 Yes
 No

Internet Service Provider

Login
 Password
 Service Name (If Required)
 Connection Mode
 Idle Timeout (In Minutes)

Internet IP Address
 Get Dynamically from ISP
 Use Static IP Address

Domain Name Server (DNS) Address
 Get Automatically from ISP
 Use These DNS Servers
 Primary DNS
 Secondary DNS

NAT (Network Address Translation)
 Enable Disable

Figure 1-5

2. Select **Yes** or **No** depending on whether your ISP requires a login. This selection changes the fields available on the Basic Settings screen.
 - **Yes.** If your ISP requires a login, select the encapsulation method. Enter the login name. If you want to change the login time-out, enter a new value in minutes.

- **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 one minute, refer to [“Troubleshooting the ISP Connection” on page 7-4.](#)

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-N modem router automatically logs you in

The following table explains the fields in the Basic Settings screen.

Table 1-2. Basic Settings screen fields

Settings		Description
Does Your ISP Require a Login?		<ul style="list-style-type: none"> • Yes • No
These fields appear only if no login is required.	Account Name (If required)	Enter the account name provided by your ISP. This might also be called the host name.
	Domain Name (If required)	Enter the domain name provided by your ISP.
These fields appear only if your ISP requires a login.	Login	The login name provided by your ISP. This is often an e-mail address.
	Password	The password that you use to log in to your ISP.
	Service Name	If your ISP provided a Service Name, enter it here.
	Connection Mode	Select the connection mode: Always on, Dial on Demand, or Manually Connect.
	Idle Timeout (In minutes)	If you want to change the Internet login time-out, enter a new value in minutes. This determines how long the wireless-N 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.

Table 1-2. Basic Settings screen fields (continued)

Settings		Description
Internet IP Address		<ul style="list-style-type: none"> • Get Dynamically from ISP. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses. • 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-N modem router to which your wireless-N modem router will connect. • Use IP Over ATM (PoA). This option is only available if your ISP does not require a log in.
Domain Name Server (DNS) Address		<p>The DNS server is used to look up site addresses based on their names.</p> <ul style="list-style-type: none"> • Get Automatically from ISP. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address. • Use These DNS Servers. If you know that your ISP does not automatically transmit DNS addresses to the wireless-N modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.
NAT (Network Address Translation)		<p>NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices.</p> <ul style="list-style-type: none"> • Enable. Usually NAT is enabled. • Disable. 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 standard routing is performed by this router. Classical routing lets you directly manage the IP addresses that the wireless-N modem router uses. Classical routing should be selected only by experienced users*
This field appears only if your ISP does not require a login.	Router MAC Address	<p>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.</p> <ul style="list-style-type: none"> • Use Default MAC Address. This is the usual setting. • Use Computer MAC address. If your ISP requires MAC authentication, you can use this setting to disguise the wireless-N modem router's MAC address with the computer's own MAC address. • Use This MAC Address. 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.

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

Configuring ADSL Settings



Note: 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.



Note: NETGEAR recommends using the Setup Wizard to select the correct country to optimize detection of the ADSL settings.

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

1. From the main menu, select ADSL Settings. The ADSL Settings screen displays.

The screenshot shows a window titled "ADSL Settings". Inside the window, there are three rows of settings. The first row is "Multiplexing Method" with a dropdown menu currently showing "LLC-BASED". The second row is "VPI" with a text input field containing the number "0". The third row is "VCI" with a text input field containing the number "35". At the bottom of the window, there are two buttons: "Apply" and "Cancel".

Figure 1-6

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

Chapter 2

Configuring Your Wireless Network and Security Settings

This chapter describes how to configure the wireless features of your wireless-N modem router. For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the modem router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.



Warning: Computers can connect wirelessly at a range of several hundred feet. This can allow others outside of your immediate area to access your network.

This chapter includes:

- [“Planning Your Wireless Network”](#)
- [“Manually Configuring Your Wireless Network” on page 2-4](#)
- [“Manually Configuring Your Wireless Security” on page 2-8](#)
- [“Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network and Security” on page 2-11](#)
- [“Wireless Guest Networks” on page 2-15](#)

Planning 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, you must know the following:
 - SSID. The default SSID for the modem router is NETGEAR.
 - The wireless mode (802.11n, 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 Configuring Your Wireless Security”](#) on page 2-8.

- Push 'N' Connect (WPS) automatically implements wireless security on the modem router while, at the same time, allowing you to automatically implement wireless security on any WPS-enabled devices (such as wireless computers and wireless adapter cards). You activate WPS by pressing a WPS button on the modem router, clicking an on-screen WPS button, or entering a PIN number. This generates a new SSID and implements WPA/WPA2 security.

To set up your wireless network using the WPS feature:

- Use the WPS button on the side of the modem router (there is also an on-screen WPS button), or enter the PIN of the wireless device.
- Make sure that all wireless computers and wireless adapters on the network are Wi-Fi certified and WPA or WPA 2 capable, and that they support WPS configuration.

See [“Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network and Security”](#) on page 2-11.

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the 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 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 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 wireless-N 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-N 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 (see [“Restricting Wireless Access to Your Network” on page 6-11](#)).
- **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 (see [“Hiding your wireless network name \(SSID\)” on page 6-12](#)).
- **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 (see [“Configuring WEP” on page 2-9](#)).
- **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 (see [“Configuring WPA-PSK \(TKIP\) + WPA2-PSK \(AES\) Security” on page 2-8](#)).

Manually Configuring Your Wireless Network

You can view or manually configure the wireless settings and wireless security for the modem router in the Wireless Settings screen. If you want to make changes, make sure to note the current settings first. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.



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

To manually configure the wireless settings:

1. Log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Wireless Settings in the main menu. The Wireless Settings screen displays.

Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: Europe

Channel: Auto

Mode: Up to 145Mbps

Security Options

None

WEP

WPA-PSK (TKIP)

WPA2-PSK (AES)


WPA-PSK (TKIP) + WPA2-PSK (AES)

Apply Cancel

Figure 2-1


Table 2-1 on page 2-6 describes the selections on the Wireless Settings screen.

3. Choose a suitable descriptive name for the wireless network name (SSID). In the **SSID** field, enter a value of up to 32 alphanumeric characters. The default SSID is **NETGEAR**.

	Note: The SSID of any wireless access adapters must match the SSID you specify in the wireless-N modem router. If they do not match, you will not get a wireless connection.
---	---

4. Select the region in which the wireless interface will operate.
5. Set the channel if necessary. The default channel is 11.

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless-N modem router. For more information about the wireless channel frequencies, see the online document that you can access from [“Preparing Your Network” in Appendix B](#).

	Note: Up to 300 Mbps mode uses two channels, but in this mode only the first channel is listed in the channel pulldown menu. The associated channels in this mode are: 1+5, 2+6, 3+7, 4+8, 5+9, 6+10, and 7+11. When you select another wireless network mode, the channel pulldown displays all available channels: 1 through 13. However, available wireless channels depend on the selected wireless region.
---	--

6. For initial configuration and test, leave the Wireless Card Access List set to allow everyone access by making sure that **Turn Access Control On** is not selected in the Wireless Station Access List. In addition, leave the encryption strength set to **None**.
7. Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.
8. Configure and test your computers for wireless connectivity.

Program the wireless adapter of your computers to have the same SSID and channel that you specified in the router. Check that they have a wireless link and can obtain an IP address by DHCP from the wireless-N modem router.

Once your computers have basic wireless connectivity to the wireless-N modem router, you can configure the advanced wireless security functions of the wireless-N modem router.

Table 2-1. Wireless Settings

Settings	Description
Name (SSID)	The SSID is also known as the wireless network name. Enter up to 32-characters in this field. This field is case-sensitive. The default SSID is NETGEAR , but NETGEAR strongly recommends that you change your network name. Any device you that want to let join a wireless network must use the SSID.
Region	The location where the wireless-N modem router is used. Select your region. This setting will apply to any guest networks you set up. It might not be legal to operate the wireless-N modem router in a region other than the regions shown here.
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 experiment with different channels to see which is best. For Up to 145 Mbps mode, the default channel is 11; for Up to 300 Mbps mode, the default channel is 7. The number of available channels varies by region and depends on the selected mode.
Mode The mode can be set only for the primary wireless LAN (NETGEAR).	<ul style="list-style-type: none"> • 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. • 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. • Up to 54 Mbps. Allows wireless stations that support speeds up to 54 Mbps.

Table 2-1. Wireless Settings (continued)

Settings	Description	
Security Options	None	Wireless security is not used.
	WEP	In WEP (Wired Equivalent Privacy) mode you can select 64-bit or 128-bit data encryption. This mode has been superseded by WPA-PSK and WPA2-PSK, which should be selected if possible. See “Configuring WEP.”
	WPA-PSK (TKIP)	WPA Pre-Shared-Key (Wi-Fi Protected Access Pre-Shared Key) uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption, implements most of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards, but not all wireless access points. See “Configuring WPA-PSK (TKIP) + WPA2-PSK (AES) Security.”
	WPA2-PSK (AES)	WPA Pre-Shared-Key (Wi-Fi Protected Access 2 with Pre-Shared Key) uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. WPA2-PSK provides the best throughput with 802.11N because the encryption is supported in the hardware. WPA2-PSK uses AES (Advanced Encryption Standard) data encryption, implements the full IEEE 802.11i standard, but does not work with some older network cards. See “Configuring WPA-PSK (TKIP) + WPA2-PSK (AES) Security.”
	WPS-PSK (TKIP) + WPA2-PSK (AES)	This setting uses both WPA-PSK and WPA2-PSK encryption. A high performance client such as the NETGEAR WN511B should connect using WPA2-PSK in order to achieve maximum performance. Wireless clients that connect to this router using WPA-PSK will run at reduced performance levels. See “Configuring WPA-PSK (TKIP) + WPA2-PSK (AES) Security.”

Manually Configuring Your Wireless Security

To set up wireless security, you can either manually configure it in the Wireless Settings screen, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security (see “Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security” on page 2-11).



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 modem router from a wired computer to make further changes.

Configuring WPA-PSK (TKIP) + WPA2-PSK (AES) Security

A high-performance client such as the NETGEAR WN511B must connect to the wireless-N modem router using WPA2-PSK to achieve maximum performance. Wireless clients that connect to the wireless-N modem router using WPA-PSK run at no more than 802.11g speed. This option allows wireless clients to use either encryption method.



Note: Not all wireless adapters support WPA or WPA2. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK (TKIP) + WPA2-PSK (AES):

1. Log in at the default LAN address of **http://192.168.0.1**, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Wireless Settings below Setup in the main menu of the wireless-N modem router.
3. Select the **WPA-PSK (TKIP) + WPA2-PSK (AES)** radio button. The Wireless Settings screen expands to include more settings.
4. Enter the pre-shared key in the **Network Key** field using between 8 and 63 characters.

Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.



Note: The procedures to configure WPA-PSK (TKIP) and WPA2-PSK (AES) are very much the same. The only difference is that you select either the **WPA-PSK (TKIP)** or **WPA2-PSK (AES)** radio button.

Configuring WEP

Wired Equivalent Privacy (WEP) security is the most basic and simplest form of wireless security. It is the most often used, but least secure of the available options. 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.

To configure WEP data encryption:

1. Log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Select Wireless Settings in the main menu.
3. In the Security Options section of the screen, select **WEP (Wired Equivalent Privacy)**. The WEP Security Encryption section displays:

The screenshot shows a web interface for configuring security options. It is titled "Security Options" and contains the following sections:

- Security Options:** A list of radio buttons for selecting a security mode: None, WEP (selected), WPA-PSK (TKIP), WPA2-PSK (AES), and WPA-PSK (TKIP) + WPA2-PSK (AES).
- Security Encryption (WEP):** Two dropdown menus: "Authentication Type" set to "Automatic" and "Encryption Strength" set to "64-bit".
- Security Encryption (WEP) Key:** A "Passphrase" text input field with a "Generate" button next to it. Below it are four rows, each with a radio button and a text input field, labeled "Key 1", "Key 2", "Key 3", and "Key 4". The "Key 1" radio button is selected.
- At the bottom of the form are "Apply" and "Cancel" buttons.

Figure 2-2


4. Select the authentication type:
 - **Automatic.** This is the default setting.
 - **Open System.**
 - **Shared Key.**
5. Select the encryption strength setting:
 - **64-bit WEP.**
 - **128-bit WEP.**
6. 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.
 - **Automatic.** Enter a word or group of printable characters in the **Passphrase** field and click **Generate**. The four key boxes are automatically populated with key values.
 - **Manual.** The number of hexadecimal digits that you must enter depends on the encryption strength setting:
 - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
 - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
7. Select the radio button for the key you want to make active.

Be sure that you clearly understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one included in Windows XP allow entry of only one key, which must match the default key you set in the wireless-N modem router.
8. Click **Save** to save your settings or click **Apply** to allow your changes to take effect immediately.



Note: When configuring the wireless-N modem router from a wireless computer, if you specify WEP settings, you will lose your wireless connection when you click **Apply**. You must then either configure your wireless adapter to match the wireless-N modem router WEP settings or access the wireless-N modem router from a wired computer to make any further changes.

Using Push 'N' Connect (WPS) to Configure Your Wireless Network and Security

If your wireless clients support Wi-Fi Protected Setup (WPS), you can use this feature to configure the wireless-N modem router's SSID and security settings and, at the same time, connect the wireless client securely and easily to the wireless-N modem router. Look for the  symbol on your client device¹ (computers that will connect wirelessly to the modem router are clients). WPS automatically configures the SSID and wireless security settings for the wireless-N modem router (if the wireless-N modem router is in its default state) and broadcasts these settings to the wireless client.

Some considerations regarding WPS are:

- WPS supports only WPA-PSK and WPA2-PSK wireless security. WEP security is not supported by WPS.
- NETGEAR's Push 'N' Connect feature is based on the Wi-Fi Protected Setup (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 additional WPS capable devices. See [“Connecting Additional Wireless Client Devices After WPS Setup”](#) on page 2-14.
- If the wireless-N modem router has already been configured manually, and either WPS-PSK or WPA2-PSK security has been enabled, a wireless client can be connected quickly and simply by using the WPS method of connecting to the wireless network. In this case, the existing wireless settings are broadcast to the WPS-capable client.

These instructions assume that you are configuring WPS on the wireless-N modem router for the first time and connecting a WPS-capable device.

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

To set up basic wireless connectivity:

1. Log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.



You can also enter either of these addresses to connect to the wireless-N modem router: **http://www.routerlogin.net** or **http://www.routerlogin.com**.

2. Select Add WPS Client (computers that will connect wirelessly to the router are clients) in the main menu. The Add WPS Client wizard screen displays.



Note: If you cannot select Add WPS Client, check to see if WPS is disabled in the Advanced Wireless Settings screen. See [“Using Static Routes”](#) on page 6-15.

3. Click **Next**. The screen changes to allow you to select the method for adding the WPS client.
4. Select the method for adding the WPS client. A WPS client can be added using the Push Button method or the PIN method.
 - **Using the Push Button.** This is the preferred method. (See [Figure 2-3](#) on page 2-12.)
 - Select the **Push Button** radio box and either press the WPS Push Button on the side of the wireless-N modem router or click the soft WPS Push Button on the screen (as shown below).
 - The wireless-N modem router tries to communicate with the client; you have 2 minutes to enable WPS from the client device using its WPS networking utility.

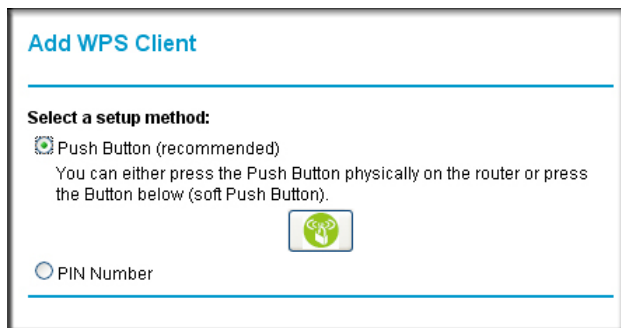


Figure 2-3

- **Entering a PIN.** If you want to use the PIN method, select the **PIN** radio box. A screen similar to the one shown below displays.
 - Go to your wireless client and, from the client's WPS utility, get the wireless client's security PIN, or follow the client's WPS utility instructions to generate a security PIN.
 - Then, enter this PIN in the **Enter Client's PIN** field provided on the wireless-N modem router and click **Apply**. You have 4 minutes to enable WPS on the router using this method.

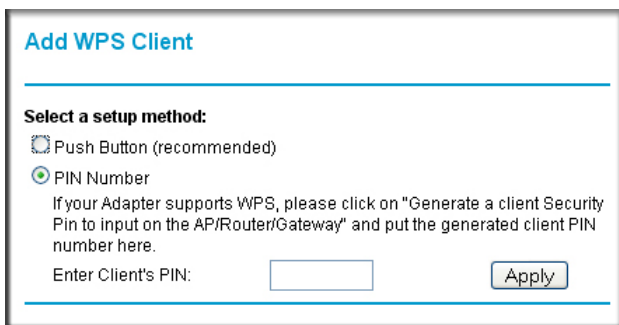



Figure 2-4

Using either method, the client wireless device will attempt to detect the WPS signal from the wireless-N modem router and establish a wireless connection in the time allotted.

- While the wireless-N modem router attempts to connect to a WPS-capable device, the Push 'N' Connect LED on the front of the wireless-N modem router blinks green. When the wireless-N modem router has established a WPS connection, the LED is solid green.
- If a connection is established, the wireless-N modem router WPS screen displays a message confirming that the wireless client was successfully added to the wireless network. (The wireless-N modem router has generated an SSID, implemented WPA/WPA2 wireless security [including a PSK security password] on the wireless-N modem router, and has sent this configuration to the wireless client.)

5. Note the new SSID and WPA/WPA2 password for the wireless network.

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

	Note: If no WPS-capable client devices are located during the 2-minute timeframe, security will not be implemented on the modem router.
---	--

Connecting Additional Wireless Client Devices After WPS Setup

You can add more WPS clients to your wireless network, or you can add a combination of WPS-enabled clients and clients without WPS.



Note: Your wireless settings remain the same when you add another WPS-enabled client, as long as the **Keep Existing Wireless Settings** checkbox is selected in the Advanced WPS Settings screen (listed under the Advanced heading in the modem router main menu). If you clear this checkbox, when you add the client, a new SSID and passphrase will be generated, and all existing connected wireless clients will be disassociated and disconnected from the modem router.

To add a wireless client device that is WPS-enabled:

1. Follow the procedures in [“Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network and Security”](#) on page 2-11.
2. To view a list of all devices connected to your modem router (including wireless and Ethernet-connected), see [“Viewing Attached Devices”](#) in Chapter 4.


For non-WPS clients, you cannot use the WPS setup procedures to add them to the wireless network. You must record, and then manually enter your security settings (see [“Manually Configuring Your Wireless Security”](#) on page 2-8).

To connect a combination of non-WPS enabled and WPS-Enabled clients to the modem router:

1. Restore the modem router to its factory default settings (press both the Wireless and WPS buttons on the side of the modem router for 5 seconds).

When the factory settings are restored, all existing wireless clients are disassociated and disconnected from the modem router.
2. Configure the network names (SSIDs), select the WPA/PSK + WPA2/PSK radio button on the Wireless Settings screen (see [“Manually Configuring Your Wireless Security”](#) on page 2-8) and click **Apply**. On the WPA/PSK + WPA2/PSK screen, select a passphrase and click **Apply**. Record this information to add additional clients.
3. 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 2](#) (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).
4. For the WPS devices that you want to connect, follow the procedures in [“Using Push 'N' Connect \(WPS\) to Configure Your Wireless Network and Security”](#) on page 2-11.

The settings that you configured in Step 2 are broadcast to the WPS devices so that they can connect to the modem router.



Note: To make sure that your new wireless settings remain in effect, verify that the **Keep Existing Wireless Settings** checkbox is selected in the Advanced WPS Settings screen.

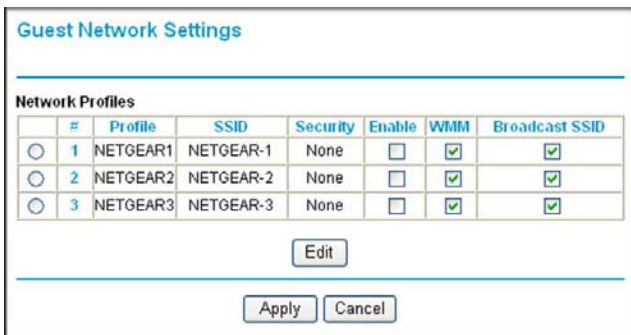
To view a list of all devices connected to your modem router (including wireless- and Ethernet-connected), see [“Viewing Attached Devices” in Chapter 4](#).

Wireless Guest Networks

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

To configure a wireless guest network:

1. In the main menu, under Setup, select Wireless Guest Network to display the following screen:



Guest Network Settings							
Network Profiles							
	#	Profile	SSID	Security	Enable	WMM	Broadcast SSID
<input type="radio"/>	1	NETGEAR1	NETGEAR-1	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/>	2	NETGEAR2	NETGEAR-2	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/>	3	NETGEAR3	NETGEAR-3	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 2-5

2. Select the radio button for the network profile that you want to set up.
3. You can specify whether the SSID broadcast is enabled, and whether you want to allow the guest to access your local network. You can also change the SSID.
 - NETGEAR strongly recommends that you change the SSID to a different name. Note that the SSID is case-sensitive. For example, GuestNetwork is not the same as Guestnetwork.

- Wireless security is disabled by default. NETGEAR strongly recommends that you implement wireless security for the guest network.
4. To configure wireless security for the guest network, enter the security options. This process is very similar to configuring wireless security for the wireless-N modem router. For more information, see [“Manually Configuring Your Wireless Security”](#) on page 2-8.
 5. When you have finished making changes, click **Apply**.

Chapter 3

Protecting Your Network

This chapter describes how to use the basic firewall features of the wireless-N modem router to protect your network. This chapter includes:

- “Protecting Access to Your Wireless-N Modem Router”
- “Blocking Keywords, Sites, and Services” on page 3-3”
- “Blocking Services” on page 3-5
- “Setting Times and Scheduling Firewall Services” on page 3-7”
- “Enabling Security Event E-mail Notification” on page 3-11

Protecting Access to Your Wireless-N Modem Router

For security reasons, the wireless-N modem router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login automatically disconnects. When prompted, enter **admin** for the wireless-N modem router user name and **password** for the wireless-N modem router password. You can use the following procedures to change the wireless-N 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 you 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.

Changing the Built-In Password

1. Log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the wireless-N modem router.



Figure 3-1

2. In the main menu, under Maintenance, select Set Password to display the following screen:

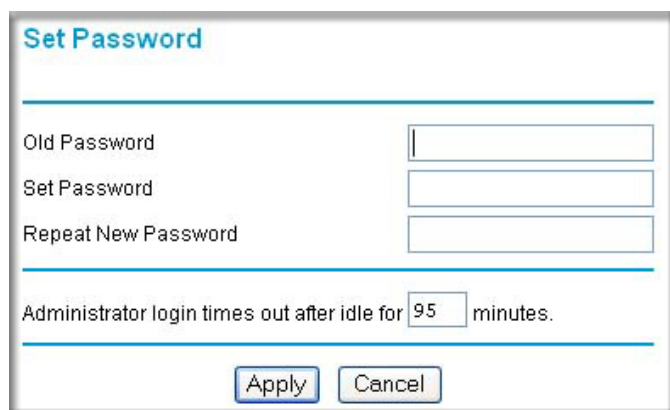
A screenshot of a web-based configuration page titled 'Set Password'. The page has a light blue header with the title. Below the title is a horizontal line. There are three input fields: 'Old Password', 'Set Password', and 'Repeat New Password'. Below these fields is another horizontal line. At the bottom, there is a text label 'Administrator login times out after idle for' followed by a text input field containing '95' and the word 'minutes.'. At the very bottom are two buttons: 'Apply' and 'Cancel'.

Figure 3-2

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



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

Changing the Administrator Login Time-out

For security, the administrator's login to the wireless-N 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.

Blocking Keywords, Sites, and Services

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

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

Blocking Sites

To block keywords and sites:

1. Log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you might have previously set for the wireless-N modem router.
2. In the main menu, under Content Filtering, select Block Sites to display the following screen:

Block Sites

Keyword Blocking

Never

Per Schedule

Always

Type Keyword or Domain Name Here.

Add Keyword

Block Sites Containing these Keywords or Domain Names:

Delete Keyword Clear List

Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address . . .

Apply Cancel

Figure 3-3

- 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.
- Enter a keyword or domain in the **Keyword** field, click **Add Keyword**, and then click **Apply**.

Some examples of keyword application follow:

- If the keyword XXX is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the keyword .com is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- Enter a period (.) as to block all Internet browsing access.

Up to 32 entries are supported in the Keyword list.

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

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

Blocking Services

To block keywords and sites:

1. Log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you might have previously set for the wireless-N modem router.
2. In the main menu, under Content Filtering, select Block Services to display this screen:

#	Service Type	Port	IP
---	--------------	------	----

Figure 3-4

3. 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.
4. click **Add** and the following screen displays:

Block Services Setup

Service Type: (dropdown)

Protocol: (dropdown)

Starting Port: (1~65534)

Ending Port: (1~65534)

Service Type/User Defined:

Filter Services For :

Only This IP Address : . . .

IP Address Range: . . .

to . . .

All IP Addresses

Figure 3-5

5. Either select a service from the Service Type drop-down list, or select **User Defined** to create a custom service.
6. Click **Add** to create the service, and the Service is listed in the Service Table:

Block Services

Services Blocking

Never

Per Schedule

Always

Service Table

#	Service Type	Port	IP
<input checked="" type="radio"/> 1	QuakeIII	27960	all

Figure 3-6

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

Setting Times and Scheduling Firewall Services

The wireless-N 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.

Setting Your Time Zone

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

1. Log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen for the wireless-N modem router.
2. Click **Schedule** below Security to display the Schedule screen.

Schedule

Days:

Every Day
 Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Time of day: (use 24-hour clock)

All Day

Start Time Hour Minute
End Time Hour Minute

Time Zone

(GMT) Greenwich Mean Time : Edinburgh, London ▾


Adjust for Daylight Savings Time
 Use this NTP Server . . .

Current Time: 2006-05-18 21:15:39

Figure 3-7

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

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

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


4. The wireless-N 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.
5. Click **Apply** to save your settings.

Scheduling 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 ([Figure 3-7](#)), 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.

Viewing, Selecting, and Saving Logged Information

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

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

Figure 3-8

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

Table 3-1. Security Log Entry Descriptions

Field	Description
Date and time	The date and time the log entry was recorded.
Description or action	The type of event and what action was taken, if any.

Table 3-1. Security Log Entry Descriptions (continued)

Field	Description
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN.
Destination	The name or IP address of the destination device or website.
Destination port and interface	The service port number of the destination device, and whether it is on the LAN or WAN.

Examples of Log Messages

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

Activation and Administration

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

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

Tue, 2006-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2

Thu, 2006-05-21 18:56:58 - Administrator logout - IP:192.168.0.2

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

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

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

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

[This entry shows when the log was 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.]

Enabling Security Event E-mail Notification

To receive logs and alerts by e-mail, you must provide your e-mail 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.

E-mail

Turn E-mail Notification On

Send alerts and logs through e-mail

Your Outgoing Mail Server:

Send to This E-mail Address

My mail server requires authentication

User Name

Password

Send Alert Immediately

When someone attempts to visit a blocked site

Send logs according to this schedule

None

Day

Time a.m. p.m.

Figure 3-9

The E-mail screen allows you to make the following selections:

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

- **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 e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this field blank, log and alert messages are not via e-mail.
- **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 the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send Logs According to this Schedule.** Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
 - Day for sending log
Specifies which day of the week to send the log. Relevant when the log is sent weekly.
 - Time for sending log
Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

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

Chapter 4

Managing Your Network

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

- “Network Management Information”
- “Backing Up, Restoring, and Erasing Your Settings” on page 4-4”
- “Automatic Firmware Recovery” on page 4-3
- “Network Management Information” on page 4-6
- “Running Diagnostic Utilities and Rebooting the Wireless-N Modem Router” on page 4-11
- “Configuring Remote Management” on page 4-12

Upgrading the Firmware

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

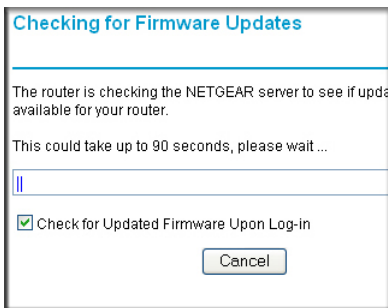


Figure 4-1



Note: To turn off the automatic firmware check at log in, clear the **Check for Updated Firmware Upon Log-in** check box on the Router Upgrade screen.

If the wireless-N modem router discovers a newer version of firmware, the message on the left displays. If no new firmware is available, the message on the right displays.

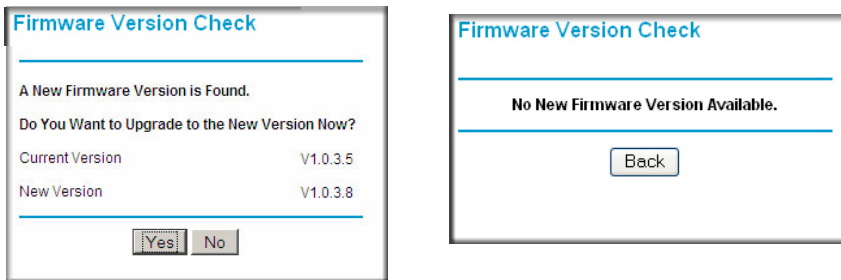


Figure 4-2

To upgrade, click **Yes** to allow the wireless-N modem router to download and install the new firmware.



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

When the upload is complete, your wireless-N modem router automatically restarts. The upgrade process could take a few minutes. Read the new firmware release notes to determine whether you must reconfigure the router after upgrading.

Manually Checking for Firmware Upgrades

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

To manually check for new firmware and install it on your wireless-N modem router:

1. Under Maintenance on the main menu, select Router Status. Note the version number of your wireless-N modem router firmware.
2. Go to the DGN2200 support page on the NETGEAR website at <http://www.netgear.com/support>.
3. If the firmware version on the NETGEAR website is newer than the firmware on your wireless-N modem router, download the file to your computer.

4. Under Maintenance on the wireless-N modem router main menu, select Router Upgrade to display the following screen:

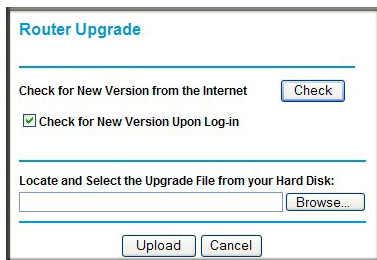



Figure 4-3

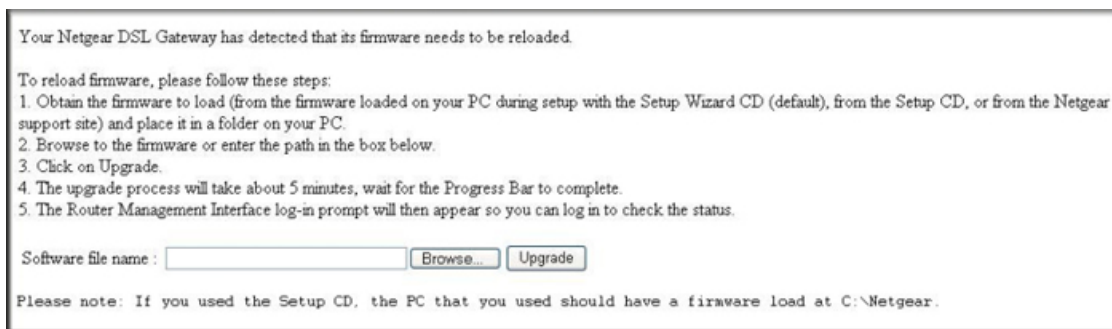
5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img or .chk).
6. Click **Upload** to send the firmware to the wireless-N modem router.

	<p>Warning: When uploading firmware to the wireless-N modem router, <i>do not</i> interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.</p>
---	---

When the upload is complete, your router automatically restarts. The upgrade process typically takes about one minute. Read the new firmware release notes to determine whether you must reconfigure the router after upgrading.

Automatic Firmware Recovery

Should the firmware become corrupted, the wireless-N modem router automatically detects this situation and opens the following screen to enable you to recover the firmware.

**Figure 4-4**

To recover the firmware:

1. If you already have the firmware file on your PC, go directly to [step 2](#). If you do not have the firmware file on your PC, obtain the firmware from the NETGEAR support site at <http://www.netgear.com/support>.
2. Click **Browse**.
3. Navigate to the firmware file. (If you used the Setup CD, recovery firmware is located in the C:\Netgear directory.)
4. Click **Upgrade**.
5. The recovery process takes about 5 minutes. Wait for the progress bar to complete. After the firmware recovery is complete, the login screen for the Smart Wizard displays, allowing you to log in to the wireless-N modem router to check its status.

Backing Up, Restoring, and Erasing Your Settings

The configuration settings of the wireless-N 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.

Backing Up the Configuration to a File

1. From the main menu, below Maintenance, select Backup Settings to display this screen:

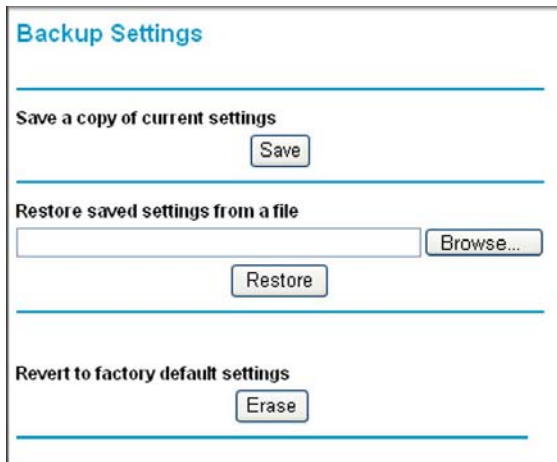


Figure 4-5

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

Restoring the Configuration from a File

1. In the main menu, below Maintenance, select Backup Settings as shown in [Figure 4-5](#).
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-N modem router.
4. The wireless-N modem router then reboots automatically.

Erasing the Configuration

Sometimes you might want to restore the wireless-N modem router to the factory default settings. This can be done by using the erase function.

1. Select Backup Settings under Maintenance in the main menu, and click the **Erase** button on the screen.
2. The wireless-N modem router then reboots automatically.

After an erase, the wireless-N modem router's password is **password**, the LAN IP address is **192.168.0.1**, and the wireless-N 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 Wireless On/Off and WPS buttons on the side panel of the wireless-N modem router simultaneously for 6 seconds.

Network Management Information

The wireless-N modem router provides a variety of status and usage information, which is discussed in the following sections.

Router Status and Usage Statistics

In the main menu, under Maintenance, select Router Status to display the Router Status screen:

Router Status	
Hardware Version	DGN2200
Firmware Version	V1.0.0.9_2.0.9
GUI Language Version	V1.0.0.14
Internet Port	
MAC Address	00:22:3F:C3:A6:D5
IP Address	68.127.106.104
Network Type	PPPoE
IP Subnet Mask	255.255.255.255
Domain Name Server	68.94.156.1 68.94.157.1
LAN Port	
MAC Address	00:22:3F:C3:A6:D4
IP Address	192.168.0.1
DHCP	ON
IP Subnet Mask	255.255.255.0
Modem	
ADSL Firmware Version	A2pB025c1.d21j2
Modem Status	Connected
DownStream Connection Speed	3008 kbps
UpStream Connection Speed	512 kbps
VPI	0
VCI	35
Wireless Port	
Name (SSID)	NETGEAR
Region	Europe
Channel	--
Mode	Up to 145 Mbps
Wireless AP	Off
Broadcast Name	Off
<input type="button" value="Show Statistics"/> <input type="button" value="Connection Status"/>	

Figure 4-6

The Router Status screen provides status and usage information, including the following settings.

Table 4-1. Router Status Fields

Component	Field	Description
	Account Name	The host name that is assigned to the wireless-N modem router in the Basic Settings screen.
	Firmware Version	This field displays the wireless-N modem router firmware version.
ADSL Port	MAC Address	This field displays the Ethernet MAC address being used by the Internet (ADSL) port of the wireless-N modem router.
	IP Address	This field displays the IP address being used by the Internet (ADSL) port of the wireless-N modem router. If no address is shown, the wireless-N modem router cannot connect to the Internet.
	Network Type	The network type depends upon your ISP.
	IP Subnet Mask	This field displays the IP subnet mask being used by the Internet (ADSL) port of the wireless-N modem router.
	Gateway IP Address	IP address used as a gateway to the Internet for computers configured to use DHCP.
	Domain Name Server	This field displays the DNS server IP addresses being used by the wireless-N modem router. These addresses are usually obtained dynamically from the ISP.
LAN Port	MAC Address	This field displays the Ethernet MAC address being used by the local (LAN) port of the wireless-N modem router.
	IP Address	This field displays the IP address being used by the local (LAN) port of the wireless-N modem router. The default is 192.168.0.1.
	DHCP	If Off, the wireless-N modem router does not assign IP addresses to PCs on the LAN. If On, the wireless-N modem router does assign IP addresses to PCs on the LAN.
	IP Subnet Mask	This field displays the IP subnet mask being used by the local (LAN) port of the wireless-N modem router. The default is 255.255.255.0.

Table 4-1. Router Status Fields (continued)

Component	Field	Description
Modem	ADSL Firmware Version	The version of the firmware.
	Modem Status	The connection status of the modem.
	DownStream Connection Speed	The speed at which the modem is receiving data from the ADSL line.
	UpStream Connection Speed	The speed at which the modem is transmitting data to the ADSL line.
	VPI	The Virtual Path Identifier setting.
	VCI	The Virtual Channel Identifier setting.
Wireless Port	Name (SSID)	The service set ID, also known as the wireless network name for WLAN1.
	Region	The country where the unit is set up for use.
	Channel	The current channel, which determines the operating frequency.
	Wireless AP	Indicates if the access point feature is enabled for WLAN1. If disabled, the Wireless LED on the front panel is off.
	Broadcast Name	Indicates if the wireless-N modem router is configured to broadcast its SSID for WLAN1.

Click the **Show Statistics** button to display wireless-N modem router usage statistics, as shown in the following screen.

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoA	1131	55	0	4	1	03:52:02
LAN	10M/100M	864	1869	0	29	13	03:52:25
WLAN	11M/54M/270M	411	0	0	7	0	03:52:21

ADSL Link	Downstream	Upstream
Connection Speed	8128 kbps	832 kbps
Line Attenuation	0.0 db	1.0 db
Noise Margin	19.7 db	6.0 db

Poll Interval: (secs)

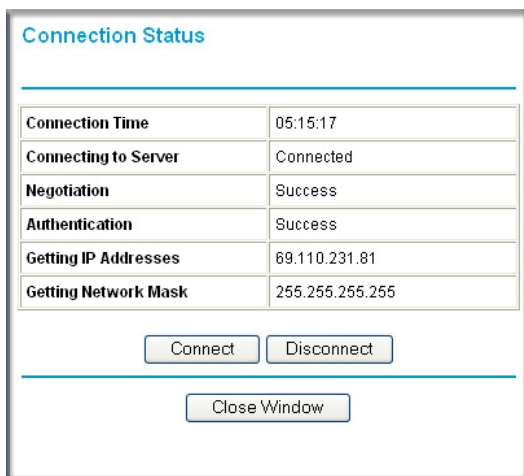
Figure 4-7

This screen shows the following statistics:

Table 4-2. Router Statistics Fields

Field	Description
WAN, LAN, or WLAN	The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
Rx B/s	The average line utilization for this port.
Up Time	The time elapsed since the last power cycle or reset.
ADSL Link Downstream or Upstream	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.
Connection Speed	Typically, the downstream speed is faster than the upstream speed.
Line Attenuation	The line attenuation increases the further you are physically located from your ISP's facilities.
Noise Margin	This is the signal-to-noise ratio and is a measure of the quality of the signal on the line.
Poll Interval	Specifies the interval at which the statistics are updated in this window. Click Stop to freeze the display.

Click the **Connection Status** button to display wireless-N modem router connection status, as shown in the following screen.

**Figure 4-8**

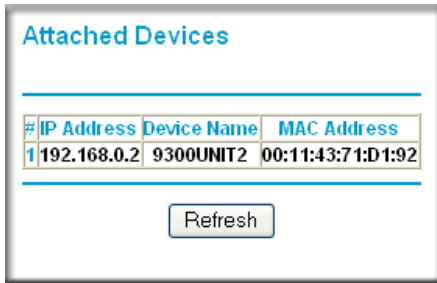
This screen shows the following statistics:

Table 4-3. Connection Status Fields (PPPoE Network Type Example)

Field	Description
Connection Time	The time elapsed since the last connection to the Internet through the ADSL port.
Connecting to sender	The connection status.
Negotiation	Success or Failed.
Authentication	Success or Failed.
Obtaining IP Address	The IP address assigned to the WAN port by the ADSL Internet Service Provider.
Obtaining Network Mask	The network mask assigned to the WAN port by the ADSL Internet Service Provider.

Viewing Attached Devices

The Attached Devices screen contains a table of all IP devices that the wireless-N modem router has discovered on the local network. In the main menu, under **Maintenance**, select **Attached Devices** to view the table, shown in the following screen.



The screenshot shows a web interface titled "Attached Devices". It contains a table with three columns: "#", "IP Address", "Device Name", and "MAC Address". The table has one row of data. Below the table is a "Refresh" button.

#	IP Address	Device Name	MAC Address
1	192.168.0.2	9300UNIT2	00:11:43:71:D1:92

Refresh

Figure 4-9

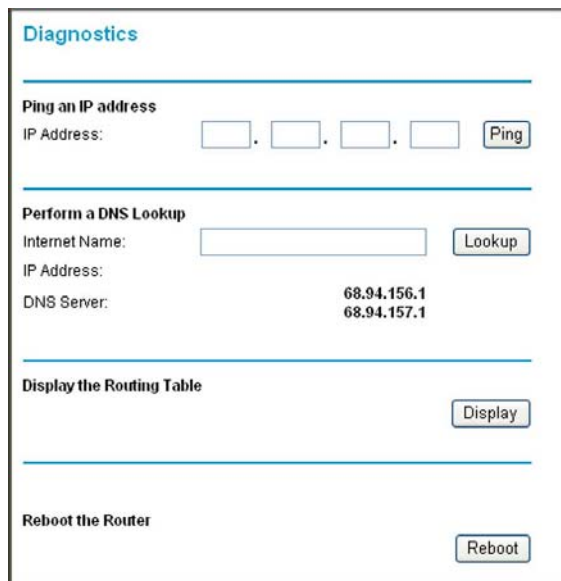
For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. Note that if the wireless-N modem router is rebooted, the table data is lost until the wireless-N modem router rediscovers the devices. To force the wireless-N modem router to look for attached devices,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

Running Diagnostic Utilities and Rebooting the Wireless-N Modem Router

The wireless-N modem router has a diagnostics feature. You can use the Diagnostics screen to perform the following functions from the wireless-N 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-N modem routers the wireless-N modem router is communicating with.
- Reboot the wireless-N modem router to enable new network configurations to take effect or to clear problems with the wireless-N modem router's network connection.

In the main menu, under Maintenance, select Diagnostics to display the following screen.



The screenshot shows the 'Diagnostics' page with the following sections:

- Ping an IP address:** A form with four input boxes for IP address segments and a 'Ping' button.
- Perform a DNS Lookup:** A form with an 'Internet Name' input box and a 'Lookup' button. Below it, the 'IP Address' is displayed as 68.94.156.1 and the 'DNS Server' as 68.94.157.1.
- Display the Routing Table:** A 'Display' button.
- Reboot the Router:** A 'Reboot' button.

Figure 4-10

Configuring Remote Management

Using the Remote Management screen, you can allow a user or users on the Internet to configure, upgrade, and check the status of your wireless-N modem router.



Note: Be sure to change the wireless-N 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. Under Advanced in the main menu, select Remote Management to display this screen:

Remote Management

Turn Remote Management On

Remote Management Address:
http://68.127.106.104:8080

Allow Remote Access By:

Only This Computer. . . .

IP Address Range From . . .
To . . .

Everyone

Port Number:

Figure 4-11

2. Select the **Turn Remote Management On** check box.
3. Specify what external addresses will be allowed to access the wireless-N modem router's remote management. For security, restrict access to as few external IP addresses as practical:
 - To allow access from any IP address on the Internet, select **Everyone**.
 - To allow access from a range of IP addresses on the Internet, select **IP address Range**. Enter a beginning and ending IP address to define the allowed range.
 - To allow access from a single IP address on the Internet, select **Only this Computer**. Enter the IP address that will be allowed access.
4. Specify the port number that will be used for accessing the management interface.

Web browser access usually uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the 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.

When accessing your wireless-N modem router from the Internet, you will type your wireless-N modem router's WAN IP address in your browser's **Address** field, followed by a colon (:)

and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter the following in your browser:

http://134.177.0.123:8080



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

Chapter 5

USB Storage

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



Figure 5-1



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

This chapter includes the following sections:

- “USB Drive Requirements” on page 5-2
- “File Sharing Scenarios” on page 5-2
- “USB Storage Basic Settings” on page 5-4
- “Configuring USB Storage Advanced Settings” on page 5-7
- “Unmounting a USB Drive” on page 5-9
- “Specifying Approved USB Devices” on page 5-10
- “Connecting to the USB Drive from a Remote Computer” on page 5-11
- “Connecting to the USB Drive with Microsoft Network Settings” on page 5-11

USB Drive Requirements

The wireless-N modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown below.

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

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

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

- The USB port on the wireless-N modem router can be used with one USB hard drive at a time. Do not attempt to use a USB hub attached to the USB port.
- Per the USB 2.0 specification, the maximum available power is 5V @ 0.5A. Some USB devices may exceed this requirement, in which case the device may not function or may function erratically. Check the documentation for your USB device to be sure.
- The wireless-N modem router supports FAT, FAT32, NTFS (read only) and Linux file systems.

File Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any PC, Mac, or Linux file type including text files, Word, PowerPoint, Excel, MP3, pictures, and multimedia. USB drive applications include:

- Sharing multimedia with friends and family — sharing MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network — storing files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and PC computers by using the USB drive as a go-between the systems.
- Sharing files with offsite coworkers — sharing files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Sharing Photos with Friends and Family

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

To share files with your friends and family:

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

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

2. If you want to specify read only access, or to allow access from the Internet, see [“Configuring USB Storage Advanced Settings”](#) on page 5-7.

Storing Files in a Central Location for Printing

This scenario is for a family that has one high quality color printer directly attached to a PC, but not shared on the local area network (LAN). This family does not have a print server:

- The daughter has some photos on her Macintosh computer that she wants to print.
- The mother has a photo-capable color printer directly attached to her PC, but not shared on the network.
- The mother and daughter’s computers are not visible to each other on the network.

How can the daughter print her photos on the color printer attached to her mother’s PC? This is where the USB drive on the wireless-N modem router can save you time and effort.

1. The daughter accesses the USB drive by typing `\\readyshare` in the address field of her Web browser. Then she copies the photos to the USB drive.
2. The mother uses a her Web browser or Microsoft Networking to transfer the files from the USB drive to the PC. Then she prints the files.

Sharing Large Files with Colleagues

Sending files that are larger than 5 MB can pose a problem for many e-mail systems. The wireless-N modem router allows you to share very large files such as PowerPoint presentations or ZIP files with colleagues at another site. Rather than tying up their mail systems with large files, your colleagues can use FTP to easily download shared files from the wireless-N modem router.

Sharing files with a remote colleague involves the following steps:

1. To protect your network, set up appropriate security. Create a user name and password for the colleague with appropriate access.

- If you want to limit USB drive access to only Read Access, from the wireless-N modem router USB Storage (Basic Settings) screen, click **Edit a Network folder**. In the Write Access field, select **admin**, and then click **Apply**.



Note: The password for admin is the same one that you use to access the wireless-N modem router. By default it is **password**.

- Enable FTP via Internet in the USB Storage (Advanced Settings) screen. See “[Configuring USB Storage Advanced Settings](#)” on page 5-7.

USB Storage Basic Settings

You can view or edit basic settings for the USB storage device attached to your wireless-N modem router. On the wireless-N modem router main menu below the USB heading, select Basic Settings. The following screen displays:

USB Storage (Basic Settings)

Network/Device Name: [\\readyshare](#)

Available Network Folders

Folder Name	Volume Name	Total Space	Free Space	Share Name	Read Access	Write Access
U:\	U Drive	982 MB	856 MB	\\readyshare\USB Storage	All - no password	All - no password

Figure 5-2

By default, the USB storage device is available to all computers on your local area network (LAN). To access your USB device from this screen, you can click the **Network/Device Name** or the **Share Name**.

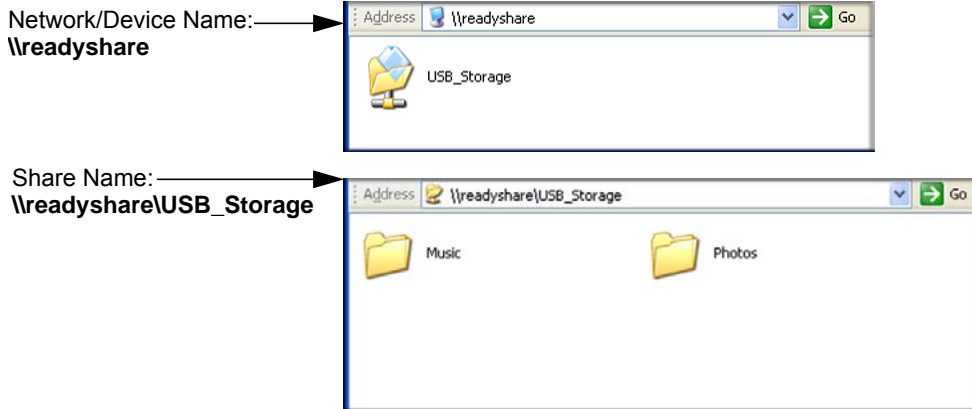


Figure 5-3

You can also type \\readyshare in the address field of your Web browser.



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

The following table explains the fields and buttons in this screen.

Table 5-1. USB Storage Basic Settings

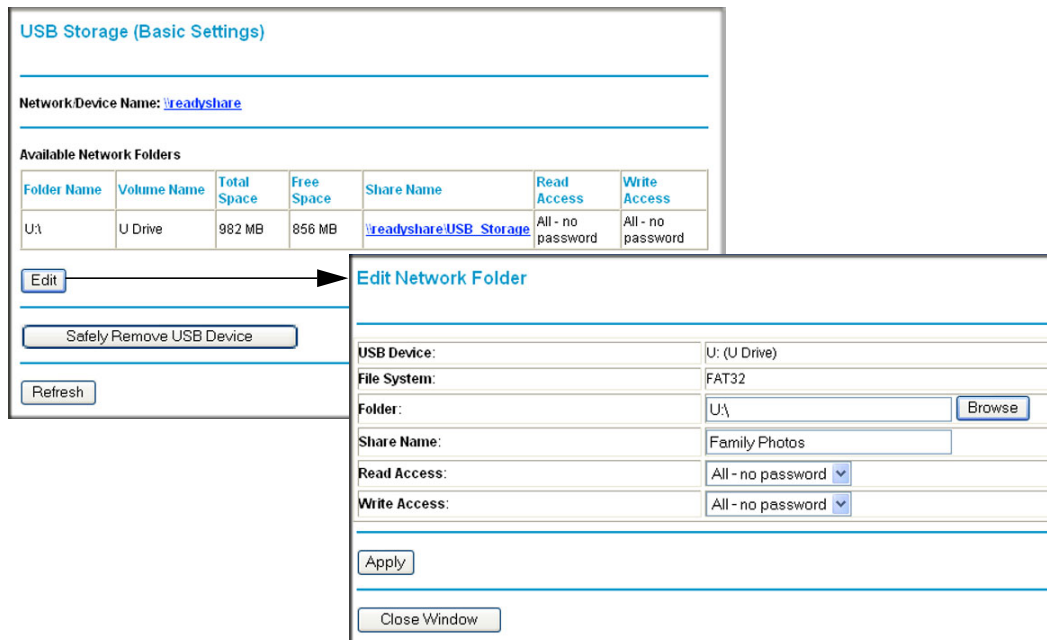
Fields and Buttons		Description
Network Device Name		The default is \\readyshare. This is the name used to access the USB device connected to the wireless-N modem router.
Available Network folders	Folder Name	Full path of the used by the Network Folder.
	Volume name	Volume name from the storage device (either USB drive or HDD).
	Total/Free Space	Shows the current utilization of the storage device.
	Share Name	<ul style="list-style-type: none"> You can click the name shown or you can type it in the address field of your Web browser. If Not Shared is shown then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.

Table 5-1. USB Storage Basic Settings (continued)

Fields and Buttons		Description
Available Network folders (continued)	Read/Write Access	<ul style="list-style-type: none"> Shows the network folder permissions/access controls. All -no password allows all users to access the network folder. admin uses the same password that you use to log in to the wireless-N modem router main menu.
Edit button		You can click the Edit button to edit the Available Network folder settings. See “ Editing a Network Folder ” on page 5-6.
Safely Remove USB Device button		Click to safely remove the USB device attached to your wireless-N modem router. See “ Unmounting a USB Drive ” on page 5-9.

Editing a Network Folder

This process is the same from either the USB Storage (Basic Settings) screen or the USB Storage (Advanced Settings) screen. Click the **Edit** button to open the Edit Network Folder screen:

**Figure 5-4**

You can use this screen to select a folder, to change the **Share Name**, or to change the **Read Access** or **Write Access** from **All-no password** to **admin**. The password for **admin** is the same one that is used to log in to the wireless-N modem router main menu. By default it is **password**.



Note: You must click **Apply** in order for your changes to take effect.

Configuring USB Storage Advanced Settings

To configure advanced USB settings, under the USB heading on the wireless-N modem router main menu, select Advanced Settings. The USB Storage (Advanced Settings) screen displays:

USB Storage (Advanced Settings)

Network/Device Name:

Workgroup:

Access Method	Status	Link	Port
Network Connection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	\\readyshare	-
HTTP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	http://readyshare/shares	80
HTTP (via internet)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		<input type="text" value="80"/>
FTP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	ftp://readyshare/shares	21
FTP (via internet)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		<input type="text" value="21"/>

Available Network Folders

Folder Name	Volume Name	Total Space	Free Space	Share Name	Read Access	Write Access
<input checked="" type="radio"/> U:\	U Drive	982 MB	856 MB	\\readyshare\USB_Storage	All - no password	All - no password

Figure 5-5

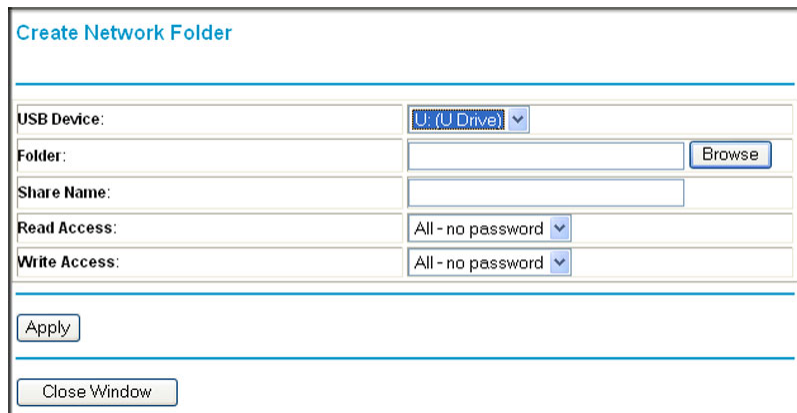
You can use this screen to specify access to the USB storage device. The following table explains the fields and buttons in the USB Storage Advanced Settings screen.

Table 5-2. USB Storage Advanced Settings

Fields		Description
Network Device Name		The default is readyshare. This is the name used to access the USB device connected to the wireless-N modem router from your computer.
Workgroup		If you are using a Windows Workgroup rather than a domain, the Workgroup name is displayed here.
Access Method	Network Connection	Enabled by default, this allows all users on the LAN to have access to the USB drive.
	HTTP	Disabled by default. If you enable this setting, you can type http://readyshare to access the USB drive.
	HTTP (via Internet)	Disabled by default. If you enable this settings, remote users can type http://readyshare to access the USB drive over the Internet.
	FTP	Disabled by default.
	FTP (via Internet)	Disabled by default. If you enable this settings, remote users can access the USB drive via ftp over the Internet.
Available Network Folders	Folder Name	Full path of the used by the Network Folder.
	Volume name	Volume name from the storage device (either USB drive or HDD).
	Total/Free Space	The current utilization of the storage device.
	Share Name	<ul style="list-style-type: none"> You can click the name shown or you can type it into the address field of your Web browser. If Not Shared is shown then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
	Read/Write Access	<ul style="list-style-type: none"> Shows the permissions/access controls on the Network Folder: All -no password allows all users to access the Network Folder. admin prompts you to enter the same password that you use to log in to the wireless-N modem router main menu.

Creating a Network Folder

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



The screenshot shows a web-based form titled "Create Network Folder". It contains several input fields and dropdown menus. The "USB Device" field is set to "U: (U Drive)". The "Folder" field is empty, with a "Browse" button to its right. The "Share Name" field is empty. The "Read Access" and "Write Access" fields are both set to "All - no password". At the bottom of the form, there are two buttons: "Apply" and "Close Window".

Figure 5-6

You can use this screen to create a folder and to specify its **Share Name**, **Read Access**, and **Write Access** from **All-no password** to **admin**. The password for **admin** is the same one that is used to log in to the wireless-N modem router main menu. By default it is **password**.



Note: You must click **Apply** in order for your changes to take effect.

Unmounting a USB Drive



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

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

Specifying Approved USB Devices

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

1. Under the Advanced Heading, select USB Settings from the main menu, and then click **Approved Devices**. The USB Drive Approved Settings screen displays:

The figure shows two screenshots of a web interface. The top screenshot is titled "USB Settings" and contains a section "Enable any USB Device connected to the USB port" with radio buttons for "Yes" (selected) and "No". To the right is a button labeled "Approved Devices". Below this is an "Apply" button. An arrow points from the "Approved Devices" button to the second screenshot. The second screenshot is titled "USB Drive Approved Devices" and features a checkbox "Allow only approved devices". Below this are two tables. The first table, "Approved USB Devices", has one row with a radio button, "UNKNOWN" volume name, "Flash Disk" device name, and "982 MB" capacity, with a "Delete" button below it. The second table, "Available USB Devices", also has one row with a radio button, "UNKNOWN" volume name, "Flash Disk" device name, and "982 MB" capacity, with an "Add" button below it. At the bottom of the second screenshot are "Apply" and "Refresh" buttons.

Figure 5-7

2. Select the USB device from the **Available USB Devices** list.
3. Click **Add**.
4. Select the **Allow only approved devices** check box.
5. Click **Apply** so that your change goes into effect.

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

Connecting to the USB Drive from a Remote Computer

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

Locating the Internet Port IP Address

The Router Status screen shows the Internet port IP address:

1. Log in to the wireless-N modem router.
2. Under the Maintenance section in the left navigator, click **Router Status**.
3. Record the IP address that is listed for the Internet Port. This is the IP address you can use to connect to the router remotely.

Accessing the Router's USB Drive Remotely Using FTP

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

1. Connect to the router by typing ftp:// and the Internet port IP address in the address field of Internet Explorer or Netscape® Navigator, for example:
ftp://10.1.65.4 If you are using dynamic DNS, you can type the DNS name rather than the IP address.
2. Type the account name and password that has access rights to the USB drive.
3. The directories of the USB drive that your account has access to will be displayed, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Connecting to the USB Drive with Microsoft Network Settings

You can access the USB drive from local computers on your home or office network using Microsoft network settings. You must be running Microsoft Windows 2000, XP, or older versions of Windows with Microsoft networking enabled. You can use normal Explorer operations such as drag and drop, file open, or cut/paste files from:

- Microsoft Windows Start Menu, Run option
- Windows Explorer

- Network Neighborhood or My Network Place

Enabling File and Printer Sharing

Each computer's network properties must be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft Networks must be enabled, as described below.



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

Configuring Windows 98SE and Windows ME

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



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

Configuring Windows 2000 and Windows XP

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

Chapter 6

Advanced Configuration

This chapter describes how to configure the advanced features of your wireless-N modem router. For information about remote management, see “[Configuring Remote Management](#)” on page 4-12. The following features are discussed in this chapter:

- “[Configuring WAN Settings](#)”
- “[Configuring Dynamic DNS](#)” on page 6-4
- “[Configuring LAN Settings](#)” on page 6-6
- “[Setting up Quality of Service \(QoS\)](#)” on page 6-9
- “[Advanced Wireless Settings](#)” on page 6-11
- “[Using Static Routes](#)” on page 6-15
- “[Configuring Universal Plug and Play](#)” on page 6-18”
- “[Building Wireless Bridging and Repeating Networks](#)” on page 6-19
- “[Port Forwarding and Port Triggering](#)” on page 6-25
- “[Traffic Meter](#)” on page 6-28

To use these features, log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever user name, password, and LAN address you have chosen for the wireless-N modem router.

Configuring WAN Settings

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

1. In the main menu, under Advanced, select WAN Setup to display the following screen.

WAN Setup

Disable SPI Firewall

Default DMZ Server

Respond to Ping on Internet Port

MTU Size (in bytes)

NAT Filtering Secured Open

Disable SIP ALG

Figure 6-1

Table 6-1. WAN Settings

Setting	Description
Disable SPI Firewall	The SPI (Stateful Packet Inspection) Firewall protects your LAN against Denial of Service attacks. This should only be disabled in special circumstances
Default DMZ Server	See “Setting Up a Default DMZ Server” on page 6-3.
Respond to a Ping on an Internet WAN Port	If you want the wireless-N modem router to respond to a ping from the Internet, select the Respond to Ping on Internet WAN Port check box. This should be used only as a diagnostic tool, since it allows your wireless-N modem router to be discovered. Do not select this check box unless you have a specific reason to do so.
MTU Size	The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes, or 1492 bytes for PPPoE connections. For some ISPs you might need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
NAT Filtering	This option determines how the router deals with inbound traffic. The Secured option provides a secured firewall to protect the PCs on LAN from attacks from the Internet, but it may cause some Internet games, point-to-point applications, or multimedia applications not to work. The Open option, on the other hand, provides a much less secured firewall, while it allows almost all Internet applications to work

Table 6-1. WAN Settings (continued)

Setting	Description
Disabling the SIP ALG	The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The Disable SIP ALG check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

Setting Up a Default DMZ Server

The default demilitarized zone (DMZ) server feature is helpful when you use some online games and videoconferencing applications that are incompatible with NAT. The wireless-N 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-N modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

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

1. In the main menu, under Advanced, select WAN Setup to display the following screen.

WAN Setup

Disable SPI Firewall

Default DMZ Server 192 . 168 . 0 . 0

Respond to Ping on Internet Port

MTU Size (in bytes) 1492

NAT Filtering Secured Open

Disable SIP ALG

Apply Cancel

Figure 6-2

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

Configuring Dynamic DNS

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

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

To configure Dynamic DNS:

1. In the main menu, under Advanced, select Dynamic DNS to display the following screen.

Figure 6-3

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 192.168.x.x or 10.x.x.x, the Dynamic DNS service will not work because private addresses will not be routed on the Internet.

Configuring 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-N modem router while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

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

- LAN IP address. 192.168.0.1
- Subnet mask. 255.255.255.0

These addresses are part of the 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 menu.

Under Advanced in the main menu, select LAN IP Setup.

LAN Setup

Device Name: DGN2200

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

Add Edit Delete

Apply Cancel

Figure 6-4

Table 6-2. LAN Setup

Setting	Description
Device Name	This is a friendly name of the router. You can see this name for the router in Network Explorer on Windows Vista systems and the Network Explorer on all Windows systems
IP Address	This is the LAN IP address of the wireless-N modem router.
IP Subnet Mask	This is the LAN subnet mask of the wireless-N modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or wireless-N modem router
Use Router as DHCP Server	See the following section “Configuring DHCP” on page 6-7
Address Reservation	See “Configuring Reserved IP Addresses” on page 6-8 .

Configuring DHCP

By default, the wireless-N 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-N 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. See the online document that you can access from [“TCP/IP Networking Basics” in Appendix B](#) for an explanation of DHCP and information about how to assign IP addresses for your network.

Use Router as DHCP Server

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

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you 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.

Configuring 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 LANSetup screen, click the **Add** button.
2. In the **IP Address** field, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.
3. Type the MAC address of the computer or server.



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

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



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

To edit or delete a reserved address entry:

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

Setting up 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.

Configuring QoS for Internet Access

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

1. To go to the QoS Setup screen, from the main menu, under Advanced, select QoS Setup.

QoS Setup

Enable WMM (Wi-Fi multimedia) settings

Turn Internet Access QoS On

Turn Bandwidth Control On

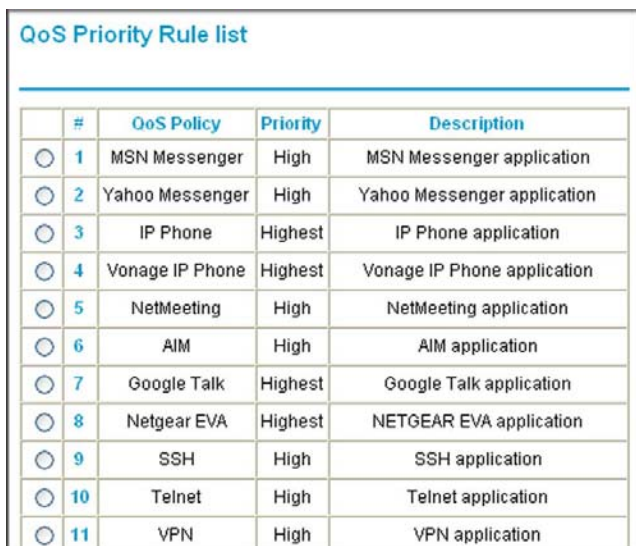
Uplink bandwidth: Maximum

Check for current Internet uplink bandwidth

QoS Priority Rule list

Figure 6-5

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



	#	QoS Policy	Priority	Description
<input type="radio"/>	1	MSN Messenger	High	MSN Messenger application
<input type="radio"/>	2	Yahoo Messenger	High	Yahoo Messenger application
<input type="radio"/>	3	IP Phone	Highest	IP Phone application
<input type="radio"/>	4	Vonage IP Phone	Highest	Vonage IP Phone application
<input type="radio"/>	5	NetMeeting	High	NetMeeting application
<input type="radio"/>	6	AIM	High	AIM application
<input type="radio"/>	7	Google Talk	Highest	Google Talk application
<input type="radio"/>	8	Netgear EVA	Highest	NETGEAR EVA application
<input type="radio"/>	9	SSH	High	SSH application
<input type="radio"/>	10	Telnet	High	Telnet application
<input type="radio"/>	11	VPN	High	VPN application

Figure 6-6

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



Figure 6-7

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

Advanced Wireless Settings

From the main menu, under the Advanced heading, select Wireless Settings to display the following screen:

Advanced Wireless Settings

Advanced Wireless Settings

Enable Wireless Router Radio

Enable SSID Broadcast

Fragmentation Length (256-2346):

CTS/RTS Threshold (1-2347):

Preamble Mode: ▾

WPS Settings

Router's PIN: **59461432**

Disable Router's PIN

Keep Existing Wireless Settings

Wireless Card Access List

Figure 6-8

Restricting Wireless Access to Your Network

By default, any wireless PC that is configured with the correct SSID can access your wireless network. For increased security, the wireless-N modem router provides several ways to restrict wireless access to your network.

You can do the following:

- Turn off wireless connectivity completely.
- Restrict access based on the wireless network name (SSID).
- Restrict access based on the Wireless Card Access List.

These options are discussed in the following sections.

Turning off wireless connectivity completely

You can completely turn off the wireless connectivity of the wireless-N modem router by pressing the Wireless On/Off button on the side panel of the wireless-N modem router. For example, if you use your notebook computer to wirelessly connect to your wireless-N modem router and you take a business trip, you can turn off the wireless portion of the wireless-N modem router while you are traveling. Other members of your household who use computers connected to the wireless-N modem router through Ethernet cables can still use the wireless-N modem router. To do this, clear the **Enable Wireless Access Point** check box on the Wireless Settings screen, and then click **Apply**.

Hiding your wireless network name (SSID)

By default, the wireless-N 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-N modem router. You must configure your wireless devices to match the wireless network name (SSID) of the wireless-N modem router.




Warning: The SSID of any wireless access adapters must match the SSID you specify in the wireless-N modem router. If they do not match, you will not get a wireless connection to the wireless-N modem router.

Restricting 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-N 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 Station Access list determines which wireless hardware devices will be allowed to connect to the wireless-N modem router.

To restrict access based on MAC addresses:

1. Log in to the wireless-N modem router at its default LAN address of **http://192.168.0.1** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

	<p>Note: If you configure the wireless-N modem router from a wireless computer, add your computer's MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the wireless-N modem router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.</p>
---	--


- In the Wireless Settings screen, under the Wireless Station Access List section, click the **Setup Access List** button to display the list.




Figure 6-9

- Select the **Turn Access Control On** check box to enable the restricting of wireless computers by their MAC addresses.
- If the wireless station is currently connected to the network, you can select it from the Available Wireless Stations list. Click **Add** to add the station to the Trusted Wireless Stations list.
- If the wireless station is not currently connected, you can enter its address manually. Enter the MAC address of the authorized computer. The MAC address is usually printed on the wireless card, or it might appear in the wireless-N modem router's DHCP table. The MAC address is 12 hexadecimal digits.

Click **Add** to add your entry. You can add several stations to the list. When you are finished adding stations, click **Apply**.

	<p>Note: You can copy and paste the MAC addresses from the wireless-N 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-N modem router. The computer should then appear in the Attached Devices screen.</p>
---	---

	Note: If you are configuring the wireless-N modem router from a wireless computer whose MAC address is not in the Trusted Wireless Stations list, and you select trusted wireless stations only, you will lose your wireless connection when you click Apply . You must then access the wireless-N modem router from a wired computer to make any further changes.
---	--

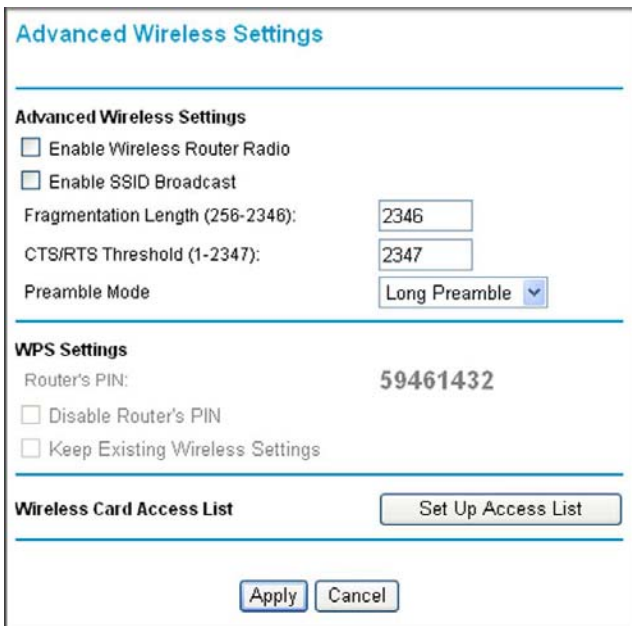
6. Make sure the **Turn Access Control On** check box is selected, and then click **Apply**.

Now, only devices on this list will be allowed to wirelessly connect to the wireless-N modem router. This prevents unauthorized access to your network.

Configuring WPS 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. Log in to the wireless-N modem router as described in “[Logging In to Your Wireless-N Modem Router](#)” on page 1-2.
2. In the main menu, under Advanced, select Advanced Wireless Settings to display the Advanced Wireless Settings screen:



Advanced Wireless Settings

Advanced Wireless Settings

Enable Wireless Router Radio

Enable SSID Broadcast

Fragmentation Length (256-2346):

CTS/RTS Threshold (1-2347):

Preamble Mode: ▾

WPS Settings

Router's PIN: **59461432**

Disable Router's PIN

Keep Existing Wireless Settings

Wireless Card Access List

Figure 6-10

By default the **Enable WPS check box** is selected. If you clear this check box and click **Apply** then you will not be able to use the Add a WPS Client feature or configure Advanced WPS settings.

3. Under WPS Settings, you can configure the following settings:

- **Disable Router's PIN.** Only when the wireless-N modem router's PIN is enabled, you can configure the wireless-N modem router's wireless settings or add a wireless client through WPS with the wireless-N modem router's PIN number. The PIN function may temporarily be disabled when the wireless-N modem router detects suspicious attempts to break into the wireless-N modem router's wireless settings by using the wireless-N modem router's PIN through WPS. You can manually enable the PIN function by deselecting 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 enabled. This will allow you to use WPS (Push 'N' Connect) to connect additional WPS capable devices to your wireless network using the existing settings.

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

Using Static Routes

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

Static Route Example

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

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

- Your company's network 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 as the wireless-N modem router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router 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 192.168.0.100. The static route setup would look like [Figure 6-12](#).

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 192.168.0.100.
- The value in the **Metric** field represents the number of routers between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.
- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

Configuring Static Routes

1. Log in to the wireless-N modem router as described in “[Logging In to Your Wireless-N Modem Router](#)” on page 1-2.
2. In the main menu, under Advanced, select Static Routes to display the Static Routes table.

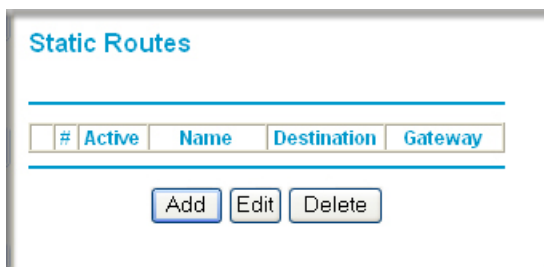


Figure 6-11

To Add a Static Route

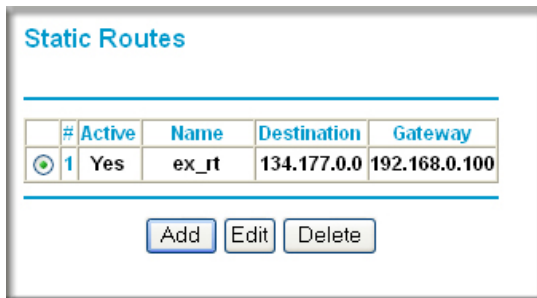
1. Click **Add** to open the following Static Routes screen.

The screenshot shows a web-based configuration interface for static routes. The title is "Static Routes". Below the title, there are several fields and checkboxes. The "Route Name" field contains "ex_rt". There are two checked checkboxes: "Private" and "Active". The "Destination IP Address" field is split into four boxes containing "134", "177", "0", and "0". The "IP Subnet Mask" field is split into four boxes containing "255", "255", "0", and "0". The "Gateway IP Address" field is split into four boxes containing "192", "168", "0", and "100". The "Metric" field contains "2". At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Figure 6-12

2. Enter a route name for this static route in the **Route Name** field. This name is for identification purpose only.
3. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Select **Active** to make this route effective.
5. Enter the destination IP address of the final destination.
6. Enter the IP subnet mask for this destination. If the destination is a single host, type 255.255.255.255.
7. Enter the gateway IP address, which must be a router on the same LAN segment as the router.
8. 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.

- Click **Apply**. The Static Routes table is updated to show the new entry.



#	Active	Name	Destination	Gateway
1	Yes	ex_rt	134.177.0.0	192.168.0.100

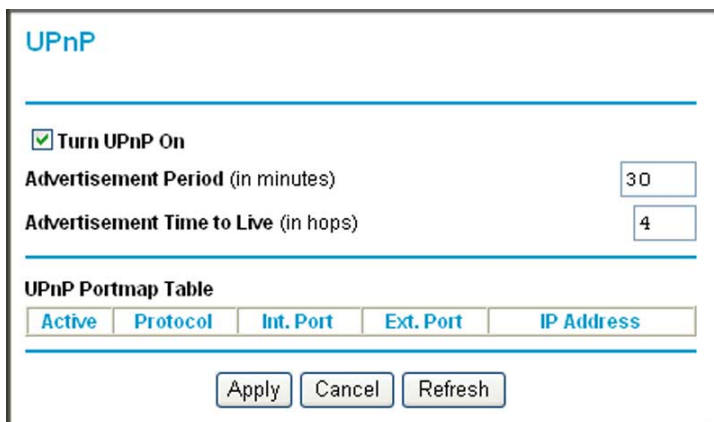
Add Edit Delete

Figure 6-13

Configuring 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.

- Select UPnP on the main menu to display the UPnP screen:



UPnP

Turn UPnP On

Advertisement Period (in minutes)

Advertisement Time to Live (in hops)

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
--------	----------	-----------	-----------	------------

Apply Cancel Refresh

Figure 6-14

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-N modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the wireless-N modem router.
- **Advertisement Period.** The advertisement period is how often the wireless-N 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-N 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-N 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.

Building Wireless Bridging and Repeating Networks

With the DGN2200 wireless-N 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-N modem router communicates with another bridge-mode wireless station. See [“Point-to-Point Bridge Configuration.”](#)
- **Multi-point bridge.** The wireless-N 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.”](#)
- **Repeater with wireless client association.** Sends all traffic to the remote access point. See [“Repeater with Wireless Client Association.”](#)



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

To view or change these configurations, select Advanced Wireless Settings from the main menu:

Wireless Repeating Function

Enable Wireless Repeating Function

Wireless MAC of this router: 00:22:3F:C3:A6:D4

Wireless Repeater

Repeater IP Address: 192 . 168 . 0 . []

Disable Wireless Client Association

Base Station MAC Address: [] . [] . [] . [] . []

Wireless Base Station

Disable Wireless Client Association

Repeater MAC Address 1: [] . [] . [] . [] . []

Repeater MAC Address 2: [] . [] . [] . [] . []

Repeater MAC Address 3: [] . [] . [] . [] . []

Repeater MAC Address 4: [] . [] . [] . [] . []

Apply Cancel

Figure 6-15

Point-to-Point Bridge Configuration

In point-to-point bridge mode, the DGN2200 wireless-N 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.

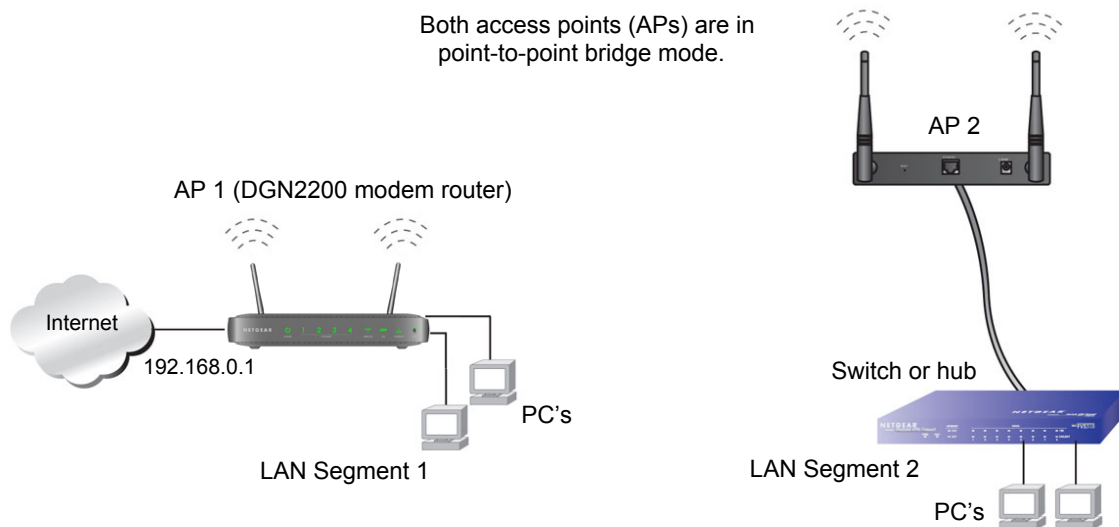


Figure 6-16

To set up a point-to-point bridge configuration (shown in [Figure 6-16](#)):

1. Configure the DGN2200 wireless-N 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 DGN2200 wireless-N modem router must have AP 2's MAC address in its **Remote MAC Address** field, and AP 2 must have the DGN2200'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 AP2. AP1 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 wireless-N modem router to bridge to multiple peer access points simultaneously. As a bridge, wireless client associations are disabled—only wired clients can be connected. Multi-point bridge mode configuration includes the following steps:

- Entering the MAC addresses of the other access points in the fields provided.
- Setting the other bridge-mode access points to Point-to-Point Bridge mode, using the MAC address of this DGN2200 as the Remote MAC Address.
- Using wireless security to protect this traffic.

The following figure shows an example of a multi-point bridge mode configuration.

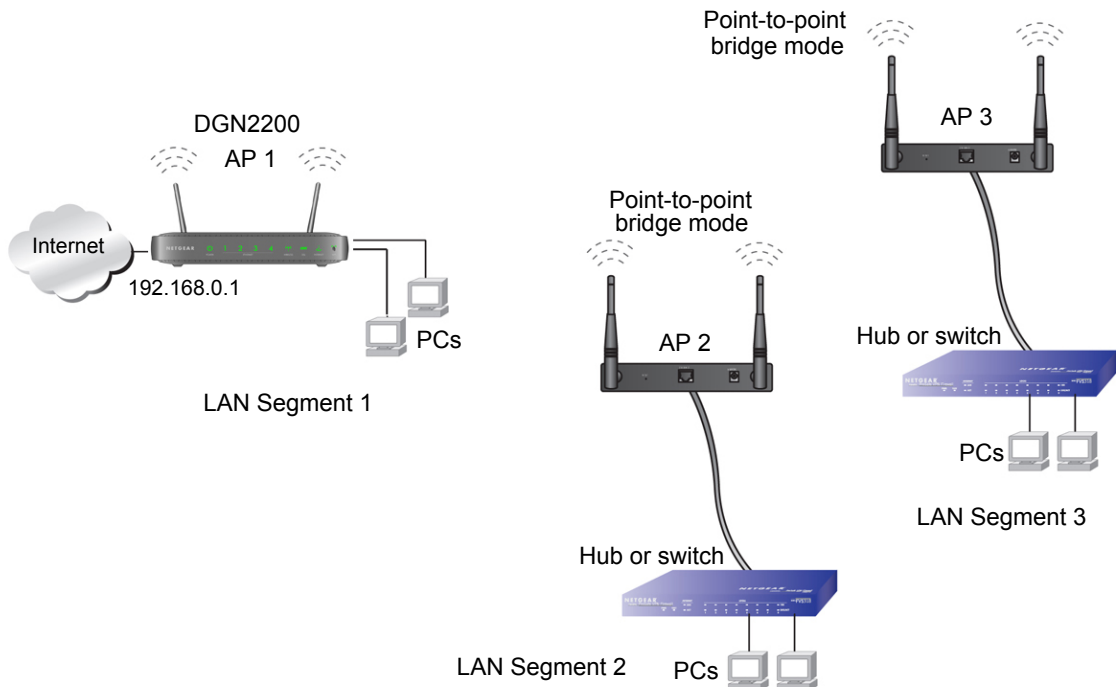


Figure 6-17

To set up the multi-point bridge configuration shown in [Figure 6-17](#):

1. Configure the operating mode of the wireless-N modem routers.
 - Because it is in a central location, configure the DGN2200 wireless-N 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 (AP2) on LAN Segment 2 in point-to-point bridge mode with the remote MAC address of the DGN2200 wireless-N modem router.
 - Configure the access point (AP3) on LAN Segment 3 in point-to-point bridge mode with the remote MAC address of the DGN2200 wireless-N modem router.
2. Disable the DHCP server on AP2 and AP3. AP1 will then be the DHCP server.
3. Verify the following for all access points:
 - The LAN network configuration of the wireless-N modem router and other access points are configured to operate in the same LAN network address range as the LAN devices.
 - Only one AP, the DGN2200 wireless-N modem router in [Figure 6-17](#), is configured in point-to-multi-point bridge mode; all the others are in point-to-point bridge mode.
 - All APs, including the DGN2200 wireless-N modem router, must be on the same LAN. That is, all the AP 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 DGN2200 wireless-N 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 DGN2200 wireless-N 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 6-17](#) will not be able to connect to the wireless-N 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 DGN2200 wireless-N modem router sends all traffic to a remote AP. For the repeater mode, you must enter the MAC address of the remote “parent” access point. Alternatively, you can configure the DGN2200 wireless-N 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 DGN2200 wireless-N modem router.
- You cannot configure a sequence of parent/child APs. You are limited to only one parent AP, although if the DGN2200 wireless-N modem router is the parent AP, it can connect with up to four child APs.

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

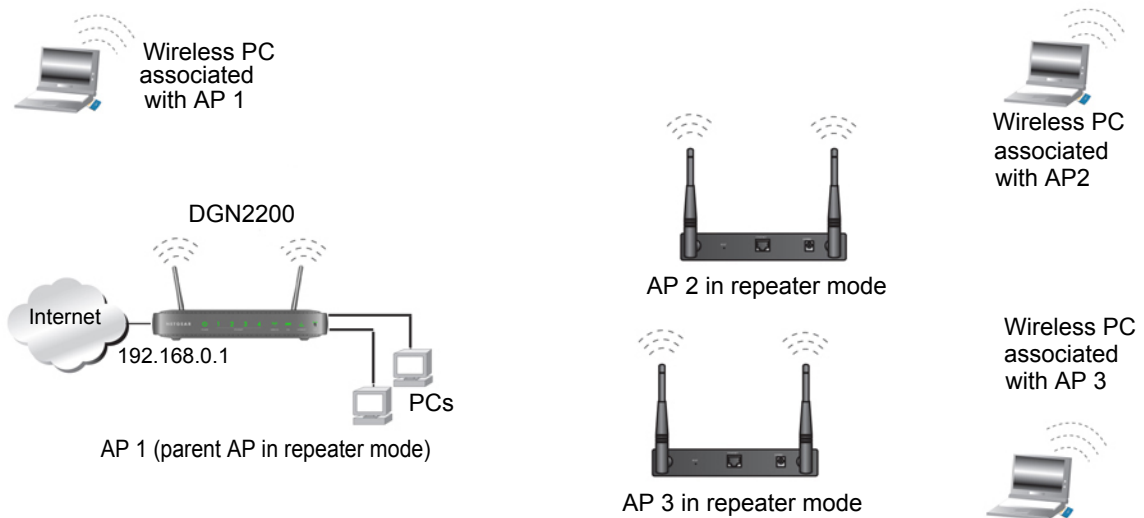


Figure 6-18

To set up a repeater with wireless client association:

1. Configure the operating mode of the devices.
 - Configure AP 1 (the DGN2200 wireless-N modem router in [Figure 6-18](#)) on 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 AP is configured to operate in the same LAN network address range as the LAN devices.
 - The APs must be on the same LAN. That is, the LAN IP addresses for the APs must be in the same network.
 - If you are using DHCP, AP devices should be set to **Obtain an IP address automatically (DHCP Client)** in the IP Address Source section of the Basic IP Settings screen.
 - AP 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.

Port Forwarding and Port Triggering

Port forwarding and port triggering are advanced features that affect the behavior of the firewall in your wireless-N modem router. Using the Port Forwarding / Port Triggering screen, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games (like Quake III), or to use Internet applications (like CU-SeeMe)

- Port triggering Port triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and triggers the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer. Port triggering allows requests from the Internet only after a designated port is triggered. Port triggering applies to chat and Internet games.
- Port forwarding is designed for FTP, Web server, or other server-based services. Once port forwarding is set up, requests from the Internet are forwarded to the proper server.

Port Forwarding

To set up port forwarding:

1. From the main menu, under the Advanced Heading, select Port Forwarding/Port Triggering. The following screen displays:

Port Forwarding / Port Triggering

Please select the service type.

Port Forwarding
 Port Triggering

Service Name: Age-of-Empire (dropdown)
Server IP Address: 192 . 168 . 0 . [] Add

#	Service Name	Start Port	End Port	Server IP Address
---	--------------	------------	----------	-------------------

Edit Service Delete Service

Add Custom Service

Figure 6-19

2. You can select a service or create a custom service.
 - Select a service from the **Service Name** drop-down list and specify the computer's IP address
 - If you want to add a service that is not in the list, click the **Add Custom Service** button. Fill in the fields in the Add Custom Service screen.

The service appears in the list.

Port Triggering

To set up port triggering:

1. From the main menu, under the Advanced Heading, select Port Forwarding/Port Triggering.
2. Select the Port Triggering Radio button to display the following screen:

Figure 6-20

3. Click **Add Service** and fill in the fields in the Add Service screen.

The service appears in the list. For more detailed information, see the Port Forwarding/Port Triggering help.

Advanced USB Settings

For added security the router can be setup to only share approved USB devices. To enable this feature, select No and click Apply.

To define the approved devices, click Approved Devices

Figure 6-21

Traffic Meter

The advanced WPS settings cannot be displayed if you have selected WEP as the security option.. To display and specify advanced WPS settings:

1. Log in to the wireless-N modem router as described in “Logging In to Your Wireless-N Modem Router” on page 1-2.
2. In the main menu, under Advanced, select Traffic Meter to display the following screen:

Traffic Meter

Internet Traffic Statistics

Enable Traffic Meter

Traffic volume control by No limit

Monthly limit (Mbytes)

Round up data volume for each connection by 0 (Mbytes)

Connection time control

Monthly limit (hours)

Traffic Counter

Restart traffic counter at 00 00 On the 1st day of each month

Traffic Control

Alert prior to reaching monthly limit 0 Mbytes/Minutes

Issue warning popup

Block all traffic

Send email

Internet Traffic Statistics

Start Date/Time: Thursday, 01 Oct 2009 00:00
 Current Date/Time: Wednesday, 21 Oct 2009 22:43
 Traffic Volume Left: No limit

Period	Connection Time (hh:mm)	Traffic Volume (Mbytes)		
		Upload Avg	Download Avg	Total Avg
Today	00:00	0.00	0.00	0.00
Yesterday	00:00	0.00	0.00	0.00
This week	00:00	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00
This month	00:00	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00
Last month	00:00	0.00 / 0.00	0.00 / 0.00	0.00 / 0.00

Figure 6-22

Table 6-3. Traffic Meter

Setting		Description
Internet Traffic Statistics	Enable Traffic Meter	Check this if you wish to record the volume of Internet traffic passing through the Router's Internet port.
	Traffic volume control by	Select this if you wish to record and restrict the volume of Internet traffic passing through the router's Internet port.
	No Limit	If this is selected specified restriction will not be applied when traffic limit is reached.
	Download only	If this is selected the specified restriction will be applied to the incoming traffic only
	Both Directions	If this is selected the specified restriction will be applied to both incoming and outgoing traffic only
	Connection time control	Select this if you wish to record and restrict the time usage of the Internet connection.
	Monthly Limit	Enter the monthly volume limit or connection time limit.
	Round up data volume for each connection by	Some ISPs charge certain amount of extra data volume when users make a new connection. If this case, enter the extra data volume here.
Traffic counter		<ul style="list-style-type: none"> Restart traffic counter determines when the traffic counter restarts. Choose the desired time and day of the month. Click Restart Counter Now to restart the Traffic Counter immediately.
Traffic control	alert	
	issue warning popup	Entering a non-zero value to make the router pop-up a warning message when the monthly data volume/ connection time limit will be reached after the configured amount is run out. Only when the Traffic Status window is opened, the pop-up message can show up.
	block all traffic	all access to the Internet will be blocked
	Send email	
Internet Traffic Statistics (data display)		<ul style="list-style-type: none"> This displays statistics on Internet traffic via the Internet port. If you have not enabled the Traffic Meter, these statistics are not available. Click the Traffic Status button if you want live update about the usage status of the Internet traffic.

Chapter 7

Troubleshooting

This chapter provides information about troubleshooting your Wireless-N 300 Modem Router DGN2200. 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.”](#)
- Have I connected the router correctly?
Go to [“Basic Functioning.”](#)
- I cannot access the router’s configuration with my browser.
Go to [“Cannot Log in to the Wireless-N Modem Router”](#) on page 7-3.
- I have configured the router but I cannot access the Internet.
Go to [“Troubleshooting the ISP Connection”](#) on page 7-4.
- I cannot remember the router’s configuration password.
Go to [“Restoring the Default Configuration and Password”](#) on page 7-10.
- I want to clear the configuration and start over again.
Go to [“Restoring the Default Configuration and Password”](#) on page 7-10.

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:
 - a. The LAN port LEDs are lit for any local ports that are connected.
 - b. 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, refer to the appropriate following section.

Welcome Page Displays instead of Router Main Menu

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

- Log into the wireless-N modem router at <http://routerlogin.com/basicsetting.htm>.
- Perform a factory reset to take the router out of "Wizard Mode" altogether.

Power LED Is Off

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

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

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

Power LED Is Red

When the router is turned on, it performs a power-on self-test. If the Power LED turns red after a few seconds or at any other time during normal operation, there is a fault within the router. The Power LED also turns red when you press the Wireless On/Off and WPS buttons on the side panel of the wireless-N modem router simultaneously for 6 seconds, and blinks red 3 times when you release these buttons. However, in this case, the wireless-N modem router is working normally.

If the Power LED turns red to indicate a router fault, turn the power off and on to see if the wireless-N modem router recovers.

If the power LED is still red 1 minute after power up:

- Turn the power off and on to see if the wireless-N modem router recovers.
- Clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.0.1. This procedure is explained in [“Using the Wireless On/Off and WPS Buttons to Reset the Router”](#) on page 7-10.

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

LAN or ADSL Port LED Is Off

If either the LAN LEDs or ADSL Link LED does not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable: when connecting the ADSL port, use the cable that was supplied with the wireless-N modem router. If the ADSL link LED is still off, this may mean that there is no ADSL service or the cable connected to the ADSL port is bad.

Window Appears Asking You to Reload Firmware

If a window appears with a message asking you to reload the firmware, this indicates that a problem has been detected with the current firmware. Please follow the on-screen instructions to access new firmware and reload the firmware into your router.

Cannot Log in to the Wireless-N Modem Router

If you are unable to log in to the wireless-N 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 192.168.0.2 to 192.168.0.254. Follow the instructions in the online document that you can access from [“Preparing Your Network”](#) in [Appendix B](#) for information about how to configure your computer.

- If your computer's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the 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 192.168.0.1. This procedure is explained in [“Using the Wireless On/Off and WPS Buttons to Reset the Router” on page 7-10.](#)
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

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

- When entering configuration settings, be sure to click the **Apply** button before moving to another 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 ISP Connection

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

ADSL Link

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

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-N 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-N 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 log-in 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 may 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-N modem router is unable to access the Internet, and your Internet LED is green or blinking green, you should determine whether the wireless-N modem router is able to obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your wireless-N 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-N modem router's configuration at <http://192.168.0.1>.
3. In the main menu, under Maintenance, click Router Status and check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your wireless-N 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-N 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. See the .

Troubleshooting PPPoE or PPPoA

The PPPoE or PPPoA connection can be debugged as follows:

1. Access the main menu of the router at <http://192.168.0.1>.
2. Under Maintenance, select **Router Status**.

3. Click the **Connection Status** button.
4. If all of the steps indicate OK, then your PPPoE or PPPoA connection is up and working.
5. If any of the steps indicates Failed, you can attempt to reconnect by clicking **Connect**. The wireless-N modem router will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. There also might be a provisioning problem with your ISP.



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

Troubleshooting Internet Browsing

If your wireless-N 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-N modem router's configuration, reboot your computer, and verify the DNS address as described in the online document that you can access from [“Preparing Your Network” in Appendix B](#). Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

If your computer obtains its information from the wireless-N modem router by DHCP, reboot the computer, and verify the wireless-N modem router address as described in the online document that you can access from [“Preparing Your Network” in Appendix B](#).

Resolving a ‘Reload Firmware’ Message

When you attempt to connect to the Internet, Windows may display a message that you must reload the router's firmware. If this situation occurs, a problem has been detected with the router's firmware.

To recover the firmware:

1. If you already have the firmware file on your PC, go directly to [step 2](#). If you do not have the firmware file on your PC, obtain the firmware from the NETGEAR support site at <http://www.netgear.com/support>.
2. Click **Browse**.
3. Navigate to the firmware file. (If you used the Setup CD, recovery firmware is located in the C:\Netgear directory.)
4. Click **Upgrade**.
5. The recovery process takes about 5 minutes. Wait for the progress bar to complete. After the firmware recovery is complete, the login screen for the Smart Wizard displays, allowing you to log in to the wireless-N modem router to check its status.

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-N 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 192.168.0.1
3. Click **OK**.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
 - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in [“LAN or ADSL Port LED Is Off”](#) on page 7-3.
 - 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-N 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-N modem router as described in the online document that you can access from [“Preparing Your Network”](#) in Appendix B.
- 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. Refer to your .

Restoring the Default Configuration and Password

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

- Use the Erase function of the Web Configuration Manager (see “[Backing Up, Restoring, and Erasing Your Settings](#)” on page 4-4).
- Press the Wireless On/Off and WPS buttons on the side panel of the router simultaneously for 6 seconds to reset the router to its factory default settings. Use this method for cases when the administration password or IP address is not known.

Using the Wireless On/Off and WPS Buttons to Reset the Router

To restore the factory default configuration settings when you do not know the administration password or IP address, you must use the Wireless On/Off and WPS buttons on the side panel of the router:

1. Press and hold the Wireless On/Off and WPS buttons simultaneously until the Power LED turns red (about 6 seconds).
2. Release the Wireless On/Off and WPS buttons. The LED blinks red three times and then turn 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-N 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.

Appendix A

Wall Mounting and Technical Specifications

This appendix provides instructions for wall mounting your router, and includes technical specifications for the Wireless-N 300 Modem Router DGN2200.

Wall-Mounting Your Modem Router

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

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

To wall mount the wireless-N modem router:

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

Holes should be 9.5 in.
(24.1 cm) center to center.

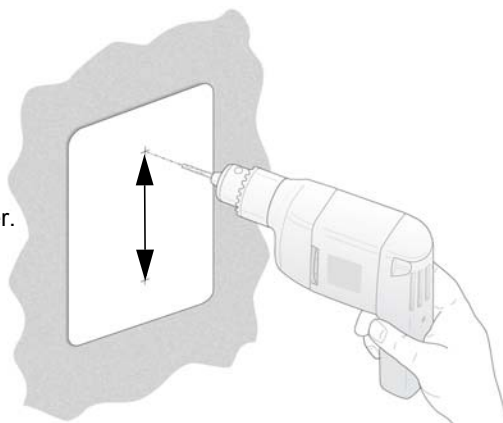


Figure A-1

2. Install wall anchors in the holes.

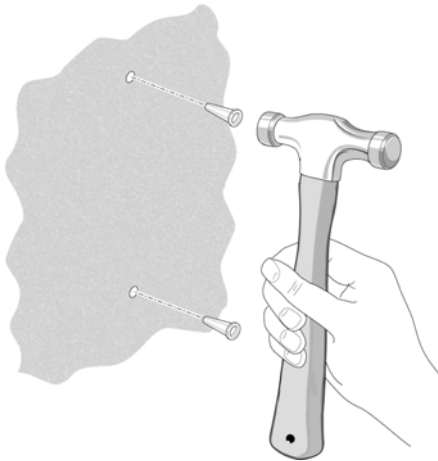


Figure A-2

Use pan head Phillips woodscrews, 3.5 x 20 mm (diameter x length, European) or #6 type screw, 1 inch long (US).

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

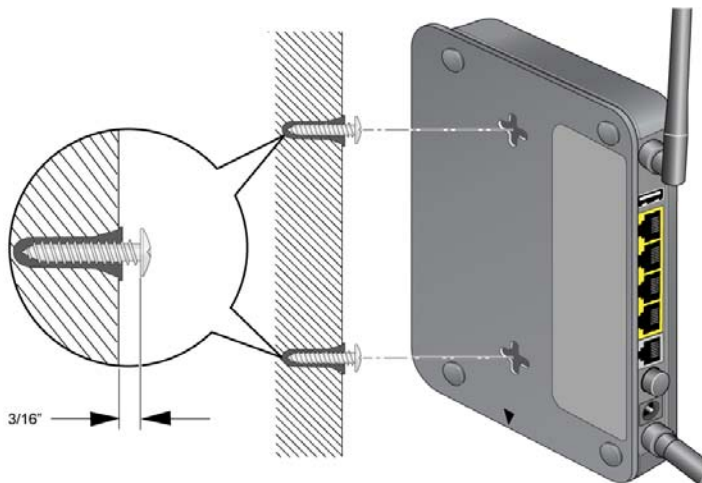


Figure A-3

4. For best wireless performance, position the wireless antennas as shown.



Figure A-4

General Specifications

Table A-1. General Specifications

Specification	Description
Network protocol and standards compatibility	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter	North America: 120V, 60 Hz, input
	UK, Australia: 240V, 50 Hz, input
	Europe: 230V, 50 Hz, input
	All regions (output): 12 V AC @ 1.0A output
Physical	Dimensions: 6.80" x 5.03" x 1.28" (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 (32° to 104° F)
	Operating humidity: 10% to 90% relative humidity, noncondensing
	Storage temperature: -20° to 70° C (-4° to 158° F)
	Storage humidity: 5 to 95% relative humidity, noncondensing

Table A-1. General Specifications (continued)

Specification	Description
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+)

Factory Default Configuration

You can use the Wireless On/Off and WPS buttons on the side panel of your router to restore factory default settings. This is called a hard reset. To perform a hard reset, push and hold the Wireless On/Off and WPS buttons simultaneously for 6 seconds. Your router will return to the factory configuration settings shown in the following table..

Table A-2. Factory Default Settings

Feature	Default Behavior	
Router Login	User login URL	http://www.routerlogin.com
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1500
	Port speed	Autosensing
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled

Table A-2. Factory Default Settings (continued)

Feature		Default Behavior
Local network (LAN) continued	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Enabled or disabled
	Time zone	PST for North America, GMT for other locations
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless	Wireless communication	Enabled
	SSID name	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	Country/region	United States (in North America; otherwise, varies by region)
	RF channel	Auto
	Operating mode	Up to 145 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open System
	Wireless card access list	All wireless stations allowed

Appendix B

Related Documents

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

Document	Link
TCP/IP Networking Basics	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Networking Basics	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing Your Network	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking Basics	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary:	http://documentation.netgear.com/reference/enu/glossary/index.htm

Numerics

128-bit WEP [2-10](#)

64-bit WEP [2-10](#)

A

access lists [6-12](#)

ADSL settings [1-9](#)

AES [2-7](#)

B

backup configuration [4-4](#)

Basic Settings screen [1-7](#)

basic wireless connectivity [2-4](#)

C

configuration

 backing up the configuration [4-4](#)

 erasing the configuration [4-5](#)

customer support [1-v](#)

D

date and time [7-10](#)

daylight savings time [3-8, 7-11](#)

default DMZ server [6-3](#)

default reset buttons [7-10](#)

Denial of Service (DoS) protection [3-3](#)

DHCP [6-7](#)

diagnostics [4-11](#)

DMZ server [6-3](#)

DNS server

 primary [1-8](#)

 primary DNS server [1-5](#)

 secondary [1-8](#)

 secondary DNS server [1-5](#)

Dynamic DNS [6-4](#)

E

ESSID [2-5](#)

F

factory settings, restoring [4-5](#)

Firmware Upgrade Assistant [1-3](#)

H

host name [1-7](#)

L

LAN IP setup menu [6-6](#)

logging in [1-2](#)

logging out [1-2](#)

M

MAC address

 MAC address being rejected [7-10](#)

 MAC address filter [6-13](#)

 MAC address spoofing [7-6](#)

 restricting wireless access by MAC address [2-9](#)

manual software upgrade [4-2](#)

metric [6-17](#)

multi-point bridge mode [6-22](#)

N

Network Time Protocol [3-7, 7-10](#)

P

passphrase [2-10](#)

password [1-4](#)

ping [6-2](#)

placement of your router [2-2](#)

plug and play [6-18](#)

point-to-point bridge mode [6-21](#)

PPPoE [1-4](#)

primary DNS server [1-5, 1-8](#)

Push 'N' Connect (WPS) [2-11](#)

R

range of your wireless connection [2-2](#)

remote management [4-12](#)

repeater mode with wireless client association [6-24](#)

reserved IP addresses [6-8](#)

reset button [7-10](#)

restore factory settings [4-5](#)

restoring your password [7-10](#)

restricting wireless access by MAC address [2-9](#)

router status [4-6](#)

S

secondary DNS server [1-5](#)

sending logs by email [3-11](#)

SMTP [3-12](#)

software, upgrading [4-1](#)

SSID [2-5](#)

syslog [3-9](#)

T

TCP/IP network troubleshooting [7-8](#)

time of day [7-10](#)

time zone [3-8](#)

timeout, administrator login [3-3](#)

time-stamping [3-8](#)

TKIP [2-7](#)

troubleshooting

 general information [7-1](#)

 network troubleshooting [7-8](#)

 troubleshooting LEDs [7-3](#)

trusted host [3-5](#)

U

updating firmware [1-3](#)

upgrading router software [4-1](#)

usage statistics [4-6](#)

USB drive requirements [5-2](#)

USB drive, unmounting [5-9](#)

USB storage [5-1](#)

W

WEP authentication [2-9](#)

Wi-Fi Protected Setup (WPS) [2-11](#)

 advanced settings [6-14](#)

 keep existing wireless settings [6-15](#)

 PIN method [2-13](#)

 push button method [2-12](#)

 router's PIN [6-15](#)

WINS [6-8](#)

wireless

 guest network [2-15](#)

wireless card access list [6-11](#)

wireless encryption

 WEP encryption [2-9](#)

wireless mode

 (up to) 145 Mbps [2-6](#)

 (up to) 300 Mbps [2-6](#)

wireless security [2-3](#)

 disabled [2-7](#)

 mixed WPS-PSK+ WPA2-PSK [2-7](#)

 WEP [2-7](#)

 WPA2-PSK [2-7](#)

 WPA-PSK [2-7](#)

WLAN [4-9](#)

World Wide Web [I-v](#)