RangeMax Wireless Router WPN824v3 User Manual

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10267-01
January 2008

Technical Support and Documentation

Please refer to the support information card that shipped with your product. When you register your product at *http://www.netgear.com/register*, we can provide you with faster expert technical support and timely notices of product and software upgrades.

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your Support information card.

E-mail: support@netgear.com

North American NETGEAR website: *http://www.netgear.com*

Setup documentation (the *Wireless Router Setup Manual*) is available on the *Resource CD*, on the support website, and on the documentation website. When the Wireless Router Model WPN824v3 is connected to the Internet, under Web Support in the main menu, select **KnowledgeBase** (to view support information) or **Documentation** (to view the most current version of this manual).

Trademarks

NETGEAR, the NETGEAR logo, ProSafe, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT and Vista are registered trademarks of Microsoft Corporation.Other brand and product names are registered trademarks or 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.

Certificate of the Manufacturer/Importer

It is hereby certified that the Wireless Router Model WPN824v3 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.

The 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.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Wireless Router Model WPN824v3 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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B 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.

Regulatory Compliance Information

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

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

Europe – EU Declaration of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328, EN301 489-17, EN60950

Europe – Declaration of Conformity in Languages of the European Community

Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES..
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, _e Radiolan spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

FCC Requirements for Operation in the United States

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model WPN824v3 Wireless Router complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

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

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

Wireless Router Model WPN824v3

Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE
PY307300071

Modifications made to the product, unless expressly approved by NETGEAR, Inc., could void the user’s right to operate the equipment.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Wireless Router Model WPN824v3) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Canada ID: 4054A-07300071

Product and Publication Details

Model Number:	WPN824v3
Publication Date:	January 2008
Product Family:	Wireless Router
Product Name:	Wireless Router Model WPN824v3
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10267-01
Publication Version Number:	1.0

Contents

About This Manual

Chapter 1
Connecting to the Internet

Chapter 2
Wireless Settings

Chapter 3
Content Filtering

About This Manual

The *NETGEAR® RangeMax™ Wireless Router WPN824v3 User Manual* provides information for configuring the features of the Wireless Router Model WPN824v3 beyond initial configuration settings. Initial configuration instructions can be found in the *Wireless Router Setup Manual*. You should have basic to 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:

Italic	Emphasis, books, CDs
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

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

➡	

💡	

⚠	

- **Scope**. This manual is written for the wireless router according to these specifications:

Product Version	Wireless Router Model WPN824v3
Manual Publication Date	January 2008

For more information about network, Internet, firewall, and VPN technologies, click the links to the NETGEAR website in Appendix B, "Related Documents."

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forward or backward through the manual one page at a time.
- A ☰ button that displays the table of contents and a ☷ button that displays an index. Double-click a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print This Manual

To print this manual, you can choose one of the following options, according to your needs.

- **Printing a page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.
- **Printing from PDF**. Your computer must have the free Adobe Acrobat Reader installed for you to view and print PDF files. The Acrobat Reader is available on the Adobe website at *http://www.adobe.com*.

- **Printing a PDF chapter.** Use the **PDF of This Chapter** link at the top left of any page.
  - Click the **PDF of This Chapter** link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
  - Click the print icon in the upper left of your browser window.
- **Printing a PDF version of the complete manual**. Use the **Complete PDF Manual** link at the top left of any page.
  - Click the **Complete PDF Manual** link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
  - Click the print icon in the upper left of your browser window.

💡

Revision History

Part Number	Version Number	Date	Description
202-10267-01	1.0	January 2008	First publication

Chapter 1
Connecting to the Internet

This chapter describes how to configure your wireless router Internet connection. When you perform the initial configuration of your wireless router using the *Resource CD* as described in the *NETGEAR Router Setup Manual*, these settings are configured automatically for you. This chapter provides further details about these settings, as well as instructions on how to log in to the wireless router for further configuration.

This chapter includes:

Using the Setup Manual

For first-time installation of your wireless router, refer to the *NETGEAR Wireless Router 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 router, modem, and computers. The Smart Wizard can 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 *User Manual* to configure additional features of your wireless router.

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

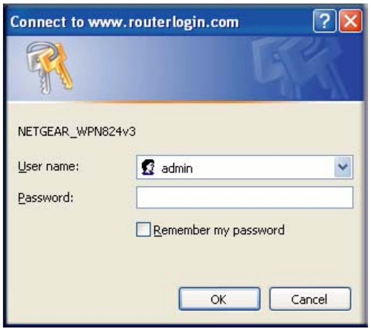
Logging In to the Wireless Router

You can log in to wireless router to view or change its settings.

To log in to the wireless router:

1. Type one of the following in the address field of your browser, and then press Enter:
   - **http://www.routerlogin.net**
   - **http://www.routerlogin.com**
   - **http://www.192.168.1.1** (the router’s IP address).

   A login screen displays.



Connect to www.routerlogin.com

NETGEAR_WPN824v3

User name: admin

Password:

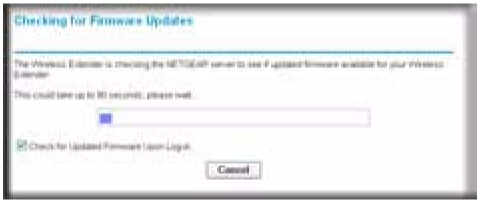
□ Remember my password

Figure 1-1

2. Enter **admin** for the router user name and **password** for the router password, both in lowercase letters. (For security reasons, the router has its own user name and password.) If you changed the user name and password from the defaults, use what you have set up.

Using Automatic Firmware Update upon Login

The Checking for Firmware Updates screen displays when you log in unless you previously cleared the **Check for Updated Firmware Upon Log-in** check box in the Router Upgrade screen (see “Router Upgrade” on page 4-12).



Checking for Firmware Updates

The Wireless Extender is checking the NETGEAR server to see if updated firmware available for your Wireless Extender.

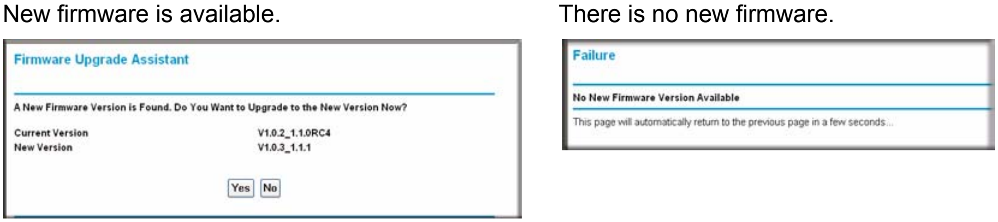
This could take up to 90 seconds, please wait...

☑ Check for Updated Firmware Upon Log-in

Figure 1-2

1. Allow the router to check for firmware updates more recent than the firmware currently installed in your wireless router.

   One of the following messages displays, depending on whether or not there is newer firmware:



New firmware is available.

Firmware Upgrade Assistant

A New Firmware Version is Found. Do You Want to Upgrade to the New Version Now?

Current Version	V1.0.2_1.1.0RC4
New Version	V1.0.3_1.1.1

There is no new firmware.

Failure

No New Firmware Version Available

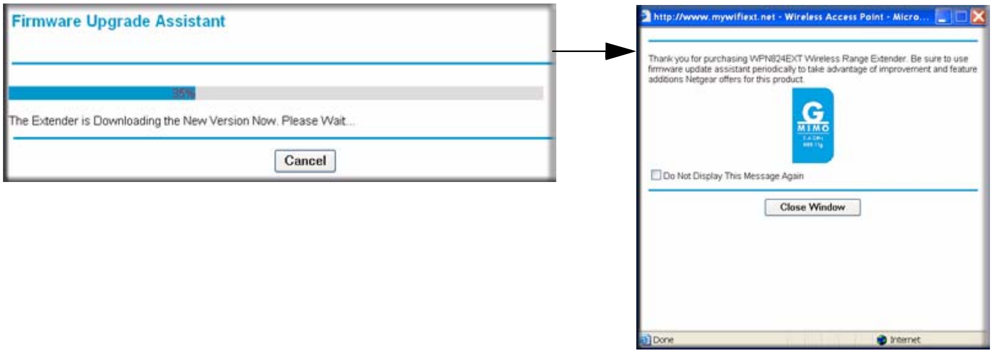
This page will automatically return to the previous page in a few seconds...

Figure 1-3

2. To download and install a newer version of firmware, click **Yes**.

   The update feature automatically installs the most recent firmware.

⚠	



Firmware Upgrade Assistant

The Extender is Downloading the New Version Now. Please Wait...

http://www.mywifiext.net - Wireless Access Point - Micro...

Thank you for purchasing WPN824EXT Wireless Range Extender. Be sure to use firmware update assistant periodically to take advantage of improvement and feature additions Netgear offers for this product.

□ Do Not Display This Message Again

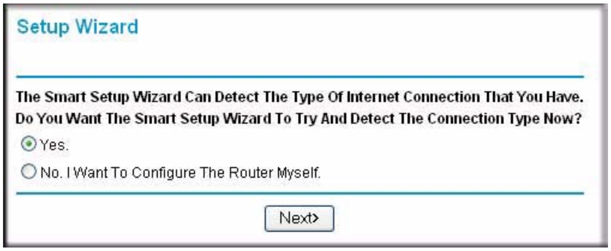
When the download is complete, a thank you screen displays, as shown in the previous figure.

Automatically Detecting Your Internet Connection

You can use the Setup Wizard to automatically detect your Internet connection.

To use the Setup Wizard:

1. Log in to the router as described in "Logging In to the Wireless Router" on page 1-2. On the main menu, select **Setup Wizard**. The following screen displays:



Setup Wizard

The Smart Setup Wizard Can Detect The Type Of Internet Connection That You Have. Do You Want The Smart Setup Wizard To Try And Detect The Connection Type Now?

● Yes.

○ No. I Want To Configure The Router Myself.

Figure 1-4

2. Select **Yes**, and click **Next**. The Setup Wizard detects your Internet connection. The Basic Settings screen displays the Internet connection settings.

3. To accept these settings, click **Apply**. If you want to change the settings, enter the settings you want in the Basic Settings screen, and then click **Apply** to save your changes. For help with the Basic Settings screen, see "Basic Settings for Your Internet Connection" on page 1-6.

Manually Setting Up Your Internet Connection

You need to prepare and have available the following before you can manually set up your router:

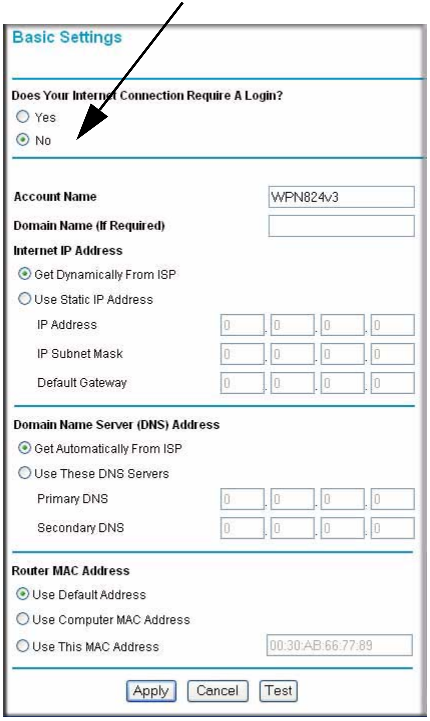
- Active Internet service.
- The Internet Service Provider (ISP) configuration information for your account.
  - ISP login name and password
  - ISP Domain Name Server (DNS) addresses
  - Fixed or static IP address
- Your computer must be set up to use DHCP to get its TCP/IP configuration from the modem router. This is usually the case. For help with DHCP, see the documentation that came with your computer, or click the link to the online document “TCP/IP Networking Basics” in Appendix B.

Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it.

Basic Settings for Your Internet Connection

You can manually view or change the Internet connection settings for your wireless router using the Basic Settings screen. Log in to the wireless router, and select **Basic Settings**:

ISP does *not* require login



Basic Settings

Does Your Internet Connection Require A Login?

○ Yes
● No

Account Name: WPN824v3

Domain Name (If Required):

Internet IP Address

● Get Dynamically From ISP
○ Use Static IP Address

IP Address: 0 . 0 . 0 . 0
IP Subnet Mask: 0 . 0 . 0 . 0
Default Gateway: 0 . 0 . 0 . 0

Domain Name Server (DNS) Address

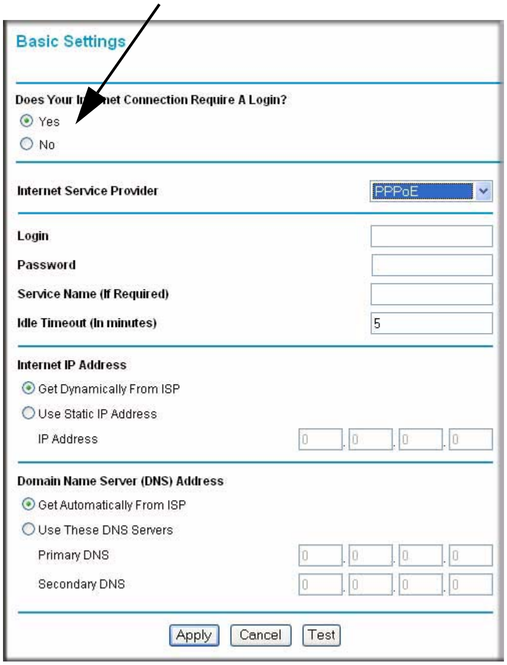
● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS: 0 . 0 . 0 . 0
Secondary DNS: 0 . 0 . 0 . 0

Router MAC Address

● Use Default Address
○ Use Computer MAC Address
○ Use This MAC Address: 00:30:AB:66:77:89

ISP *does* require login



Basic Settings

Does Your Internet Connection Require A Login?

● Yes
○ No

Internet Service Provider: PPPoE

Login:
Password:
Service Name (If Required):
Idle Timeout (In minutes): 5

Internet IP Address

● Get Dynamically From ISP
○ Use Static IP Address

IP Address: 0 . 0 . 0 . 0

Domain Name Server (DNS) Address

● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS: 0 . 0 . 0 . 0
Secondary DNS: 0 . 0 . 0 . 0

Figure 1-5

The following table explains the fields on the Basic Settings screen. Note that the group of fields included in this screen depends on whether or not a login is required.

Table 1-1. Basic Settings

Settings		Description
Does Your ISP Require a Login?		• Yes • No
These fields appear only if no login is required.	Account Name	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.	Internet Service Provider	• PPPoE • PPTP • Telstra Bigpond
	Login	The login name provided by your ISP. This is often an e-mail address.
	Service Name (If Required)	If your ISP provided a service name, enter it here. Otherwise leave this field blank.
	Idle Timeout (In Minutes)	If you want to change the login time-out, enter a new value in minutes. This determines how long the wireless router keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of zero means never log out.
Internet IP Address		• **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses. • **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 router to which your wireless router will connect.
Domain Name Server (DNS) Address		The DNS server is used to look up site addresses based on their names. • **Get Dynamically from ISP**. Your ISP uses DHCP to assign your DNS servers automatically. • **Use Static IP Address**. If you know that your ISP does not automatically transmit DNS addresses to the wireless 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.

Table 1-1. Basic Settings (continued)

Settings		Description
This field appears only if no login is required.	Router MAC Address	The Ethernet MAC address that will be used by the wireless router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then accept traffic only from the MAC address of that computer. This feature allows your wireless router to masquerade as that computer by "cloning" its MAC address. • **Use Default Address**. Use the default MAC address. • **Use Computer MAC Address**. The wireless router will capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. • **Use This MAC Address**. Enter the MAC address that you want to use.

How the Internet Connection Works

Your wireless router is configured to provide Internet access for your network. Your wireless router automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as dial-up networking or Enternet to connect, log in, or disconnect. The wireless router performs these functions automatically as needed.

To access the Internet from any computer connected to your wireless router, launch an Internet browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the wireless router's Internet light blink, indicating communication to the ISP. The browser should begin to display a Web page.

Chapter 2
Wireless Settings

This chapter describes how to configure the wireless features of your wireless router. Set up wireless features for the wireless router in this order:

1. Connect the wireless router, and get the Internet connection working, as described in Chapter 1, "Connecting to the Internet." The wireless router should work with an Ethernet LAN connection before you set up the wireless features.
2. Plan the location for the wireless router based on considerations in "Placement and Range Guidelines."
3. Configure the basic wireless settings and verify wireless connectivity, described in "Viewing or Changing Wireless Settings" on page 2-4.
4. Set up wireless security as described in "Wireless Security" on page 2-6.
5. If you want to use advanced wireless settings, see "Advanced Wireless Settings" on page 2-10.

For more information about wireless technology, click the link to the online document "Wireless Networking Basics" in Appendix B.

Placement and Range Guidelines

In planning your wireless network, select the physical placement of your wireless router in order to maximize the network performance. The operating distance or range of your wireless connection can vary significantly based on the location of the wireless router. Select a location to maximize performance. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

➡	

When used on a metallic surface, multiple input, multiple output (MIMO) units must be oriented vertically for proper operation.

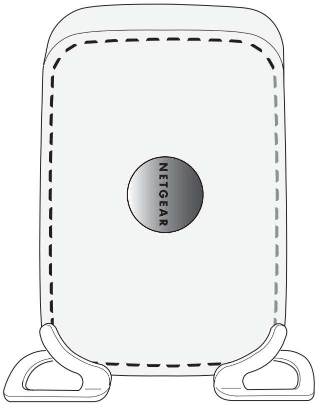


Figure 2-1

For best results, place your wireless router:

- Near the center of the area in which your computers will operate.
- In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
- Away from sources of interference, such as computers, microwave ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

Information to Record before Changing Wireless Settings

Before changing wireless settings, NETGEAR recommends that you write them down. For an existing wireless network, the person responsible for the network can provide this information. Otherwise, you choose the settings for your wireless network. Either way, record the settings for your wireless network on the following page.

Wireless Settings Form

Print this page and record your wireless settings in the spaces provided.

- **Type of service**.
  - **Cable modem service**. Use the computer you first registered with your cable ISP.
  - **DSL service**. DSL login name/e-mail address. ____________________________________

    Password. _____________________________________
- **Wireless network name (SSID)**. ________________________________ The SSID identifies the wireless network. It can be up to 32 alphanumeric characters, and *is* case-sensitive. The wireless adapter card SSID must match the SSID of the wireless router. In some configuration utilities (such as in Windows XP), the term "wireless network name" is used instead of SSID.
- **If WEP authentication is used**. Circle one: **Open System**, **Shared Key**, or **Auto**.

➡

  - **WEP encryption key size**. Choose one: **64-bit** or **128-bit**. Again, the encryption key size must be the same for the wireless adapters and the wireless router.
  - **Data encryption (WEP) keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.
    - **Passphrase method**. ________________________________ These characters *are* case-sensitive. Enter a word or group of printable characters, and click the **Generate Keys** button. Not all wireless devices support the passphrase method.
    - **Manual method**. These values *are not* case-sensitive. For 64-bit WEP, enter 10 hex digits (any combination of 0–9, A–F, or a–f). For 128-bit WEP, enter 26 hex digits.

    Key 1. _____________________________________

    Key 2. _____________________________________

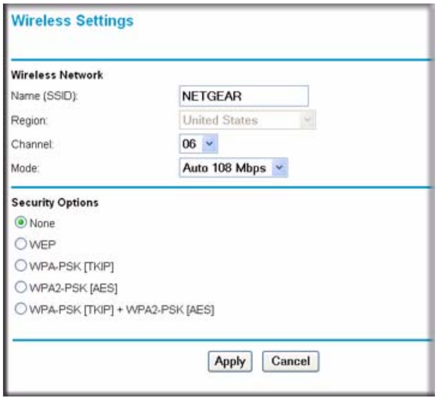
    Key 3. _____________________________________

    Key 4. _____________________________________
- **WPA-PSK authentication (if used)**. **Passphrase**. ________________________________ These characters *are* case-sensitive. Enter a word or group of printable characters. When you use WPA-PSK, other devices in the network cannot connect unless they are set to WPA-PSK and are configured with the correct passphrase.

Viewing or Changing Wireless Settings

You can view or change the wireless settings for the wireless router. If you want to make changes, make sure to note the current settings first.

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. Select **Wireless Settings** from the main menu to display the Wireless Settings screen:



Wireless Settings

Wireless Network

Name (SSID):	NETGEAR
Region:	United States
Channel:	06
Mode:	Auto 108 Mbps

Security Options

● None

○ WEP

○ WPA-PSK [TKIP]

○ WPA2-PSK [AES]

○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Figure 2-2

The settings for this screen are explained in "Understanding Wireless Settings" on page 2-5.

3. Select the region in which the router will operate.
4. For initial configuration and test, leave the other settings unchanged.
5. To save your changes, click **Apply**.
6. Configure and test your computers for wireless connectivity.
   - If you are using NETGEAR wireless adapters, they display a list of available wireless networks. While wireless security is disabled, select yours from the list, and connect.

- If you are using non-NETGEAR wireless adapters, program them with the same SSID and channel as those specified for the router. Check that they have a wireless link and can obtain an IP address by DHCP from the router.

Understanding Wireless Settings

The following table describes the fields on the Wireless Settings screen.

Table 2-1. Wireless Settings

	Description
Name (SSID)	The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. The characters are case-sensitive. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a wireless network must use the SSID.
Region	The location where the router is used.
Channel	The wireless channel used by the gateway. The default is Channel 6. Do not change the wireless 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 the best.
Mode	• **Auto 108 Mbps** (default). All 802.11g, 802.11b, and NETGEAR 108 Mbps wireless stations can connect. • **b only**. All 802.11b wireless stations can connect. 802.11g wireless stations can still be used if they can operate in 802.11b mode. • **g only**. Only 802.11g wireless stations can connect. • **b and g**. Both 802.11g and 802.11b wireless stations can connect.
Security Options	• **None**. Wireless security is disabled. This makes it easier to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security. • **WEP (Wired Equivalent Privacy)**. WEP security uses encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. • **WPA-PSK (TKIP)**. This data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA makes it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability might be limited in older equipment. • **WPA2-PSK (AES)**. Allow only computers configured with WPA2-PSK security to connect to the wireless router. • **WPA-PSK (TKIP) + WPA2-PSK (AES)**. Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the wireless router.

Wireless Security

Unlike wired network data, your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless router provides highly effective security features, which are covered in detail in this chapter, along with setting up and testing your basic connectivity.

The following figure illustrates wireless security options.

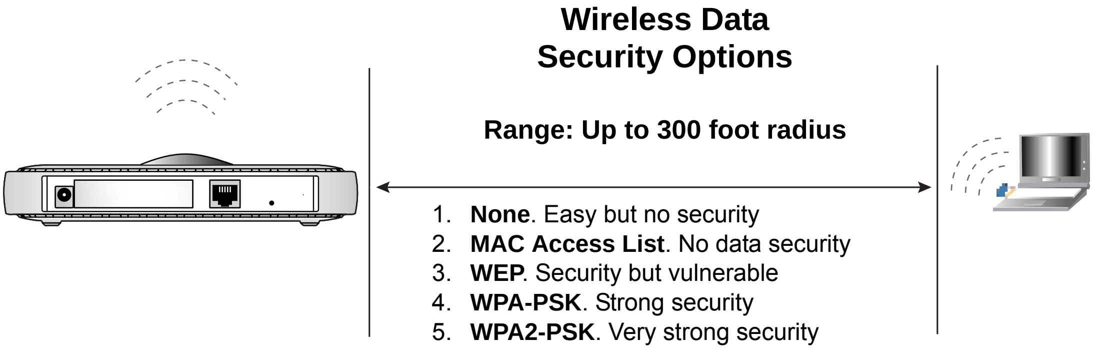

Wireless Data
Security Options
Range: Up to 300 foot radius
1. None. Easy but no security
2. MAC Access List. No data security
3. WEP. Security but vulnerable
4. WPA-PSK. Strong security
5. WPA2-PSK. Very strong security

Figure 2-3

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

- **Restrict access based on MAC address**. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the wireless router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For more information, see "Setting Up an Access List" on page 2-11.
- **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 the wireless network "discovery" feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. For more information, see "Advanced Wireless Settings" on page 2-10.

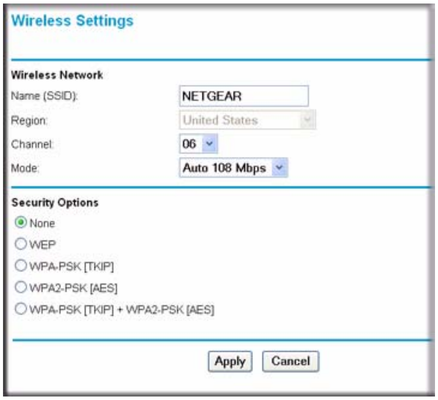
- **WEP**. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. For more information, see "Configuring WEP" on page 2-9.
- **WPA-PSK** and **WPA2-PSK**. Wi-Fi Protected Access–Pre-Shared Key (WPA-PSK) data encryption provides strong data security and blocks eavesdropping. Because these are new standards, wireless device driver and software availability might be limited. For more information, see "Configuring WPA" on page 2-7.
- **Turn off the wireless LAN**. If you disable the wireless LAN, wireless devices cannot communicate with the router at all. You might choose to turn off the wireless LAN when you are away and others on the network all use wired connections. For more information, see "Advanced Wireless Settings" on page 2-10.

Configuring WPA

To configure wireless security:

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.

2. Select **Wireless Settings** from the main menu. The Wireless Settings screen displays:



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: 06

Mode: Auto 108 Mbps

Security Options

● None

○ WEP

○ WPA-PSK [TKIP]

○ WPA2-PSK [AES]

○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Figure 2-4

3. Select the radio button for the security option of your choice.

   The fields displayed on the screen depend on which security option you select.

4. For WPA-PSK or WPA2-PSK, enter the passphrase.

5. If prompted, enter the settings for the RADIUS server. These settings are required for communication with the primary RADIUS server. You can configure a secondary RADIUS server, which is used if the primary Radius server fails.

   - **Primary Radius Server IP Address**. The IP address of the RADIUS server. The default is 0.0.0.0.
   - **Radius Port**. Port number of the RADIUS server. The default is 1812.
   - **Shared Key**. This is shared between the wireless access point and the RADIUS server during authentication.

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

Configuring WEP

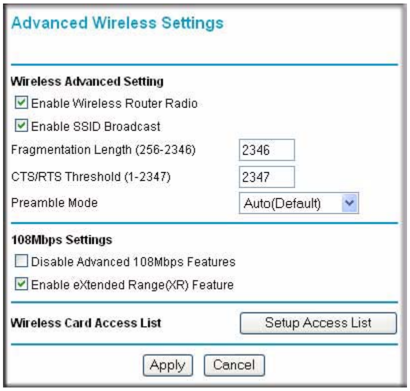
Wired Equivalent Privacy (WEP) is an older security standard than WPA and is easier to compromise. Use this type of security only if one or more of your wireless devices do not support WPA or WPA2 security.

To configure WEP data encryption:

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. From the main menu, select **Wireless Settings**. The Wireless Network screen displays.
3. Depending on the encryption strength that you want, select one of these options:
   - **WEP (Wired Equivalent Privacy) 64-bit encryption**. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
   - **WEP (Wired Equivalent Privacy) 128-bit encryption**. Enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
4. Select the authentication type. Select **Automatic**, **Open System**, or **Shared Key**. The default is Open System.
5. Enter the Security Encryption (WEP Key) settings:
   - **Passphrase**. To use a passphrase to generate the keys, enter a passphrase, and click **Generate**. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the wireless router.
   - **Key 1–Key4**. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
   - Select which of the four keys will be the default. Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected.
6. Click **Apply** to save your settings.

Advanced Wireless Settings

To specify the advanced wireless settings of your wireless router, select **Wireless Settings** under Advanced on the main menu. The Advanced Wireless Settings screen displays:



Advanced Wireless Settings

Wireless Advanced Setting

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

Fragmentation Length (256-2346) 2346

CTS/RTS Threshold (1-2347) 2347

Preamble Mode Auto(Default)

108Mbps Settings

□ Disable Advanced 108Mbps Features

☑ Enable eXtended Range(XR) Feature

Wireless Card Access List

Figure 2-5

The following table describes the settings on this screen.

Table 2-2. Advanced Wireless Settings

Settings	Description
Enable Wireless Access Point	• Selected by default, this setting enables the wireless radio, which allows the wireless router to work as an access point. • Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting. When it is off, stations cannot connect wirelessly.
Enable SSID Broadcast	• Selected by default. The wireless router broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the correct SSID. • If you disable broadcast of the SSID, only devices with the correct SSID can connect. This nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. For this reason NETGEAR recommends that you also enable wireless security.
Fragmentation Length (256–2346)	The maximum packet size used for fragmentation. Packets larger than the size entered in this field will be fragmented. The Fragment Length value must be larger than the RTS Threshold value. For best performance, leave this at the default setting (2346).

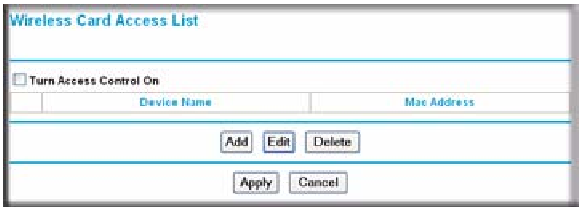
Table 2-2. Advanced Wireless Settings (continued)

Settings	Description
CTS/RTS Threshold (1–2347)	This setting is reserved for wireless testing and advanced configuration only. For best performance, leave this at the default setting (2347).
Preamble Mode	For best performance, leave this at the default setting of Auto. The other selections are Short Preamble and Long Preamble. This setting is reserved for wireless testing and advanced configuration only.
Disable Advanced 108 Mbps Features	If this check box is selected, the wireless router does not perform data compression, packet bursting, or large frame support. For the best performance, leave this at the default setting (not selected).
Enable eXtended Range (XR) Feature	This technology, eXtended Range(XR), requires no additional configuration and provides significantly longer range over 802.11 by maintaining connectivity when signals encounter barriers. For the best performance, leave this at the default setting (selected).
Turn Access Control On	Access control is disabled by default so that any computer configured with the correct SSID can connect to the wireless router. For increased security, you can restrict access to the wireless network to allow only specific computers based on their MAC addresses. See the following section, "Setting Up an Access List."

Setting Up an Access List

To turn access control on:

1. On the Advanced Wireless Settings screen, click **Setup Access List**. The Wireless Card Access List screen displays.



Wireless Card Access List

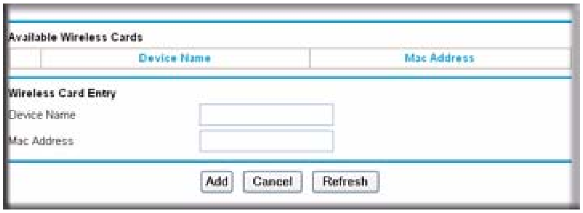
□ Turn Access Control On

	Device Name	Mac Address

Figure 2-6

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

3. Use the **Add**, **Edit**, and **Delete** buttons to add wireless computers to the list and to edit or delete access control settings. The Available Wireless Cards screen displays:.



Available Wireless Cards

	Device Name	Mac Address

Wireless Card Entry

Device Name

Mac Address

Figure 2-7

➡

Do one of the following:

- If a wireless computer is in the Available Wireless Cards list, you can capture its MAC address and add it to your list.
- You can manually enter the information for the PC.

➡

4. Click **Apply** to save changes and return to the Wireless Settings screen.

Chapter 3
Content Filtering

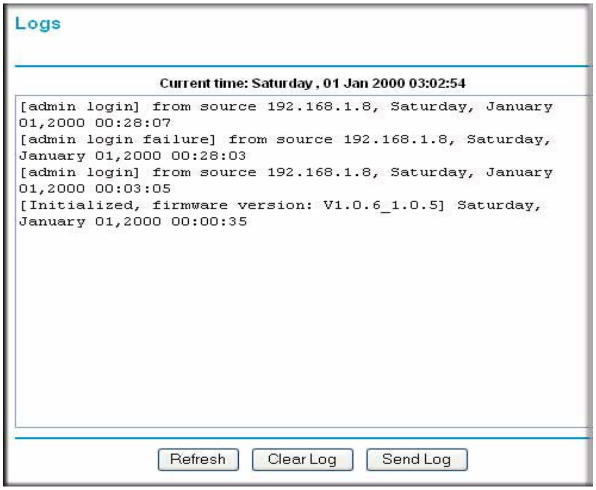
The wireless router provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time of day, Web addresses, and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

This chapter describes how to use the Web content filtering features you can configure or view by selecting the items under Content Filtering in the main menu of your router.

Logs

The log is a detailed record of which websites you have accessed or attempted to access. Up to 128 entries are stored in the log. If you have e-mail notification on, you can also receive these logs in an e-mail message (see "Enabling Security Event E-mail Notification" on page 4-9).

To view the Logs screen, log in to the wireless router. Select **Logs** under Content Filtering in the main menu.



Current time: Saturday , 01 Jan 2000 03:02:54

```
[admin login] from source 192.168.1.8, Saturday, January
01,2000 00:28:07
[admin login failure] from source 192.168.1.8, Saturday,
January 01,2000 00:28:03
[admin login] from source 192.168.1.8, Saturday, January
01,2000 00:03:05
[Initialized, firmware version: V1.0.6_1.0.5] Saturday,
January 01,2000 00:00:35
```

Figure 3-1

Log entries include these types of information:

- **Blocked** or **allowed**. If you have set up content filtering (see "Schedule" on page 3-7) text displays describing whether the access was blocked or allowed.
- **Source IP**. The name or IP address of the website or newsgroup visited or attempted to access.
- **Date and time**. The date and time the log entry was recorded.

Click a button to perform one of these actions:

- **Refresh**. Refresh the log screen.
- **Clear Log**. Clear the log entries.
- **Send Log**. E-mail the log immediately.

Blocking Sites

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

- Use keywords to block HTTP traffic.
- Use outbound service blocking to limit access from your LAN to Internet locations or services that you specify as off-limits.
- Use denial of service (DoS) protection to automatically detect and thwart DoS attacks such as Ping of Death, SYN flood, LAND Attack, and IP spoofing.
- Block unwanted traffic from the Internet to your LAN.

The following sections in this chapter explain how to configure your wireless router to perform these functions.

Blocking Keywords and Sites

You can use the wireless router to restrict access to Internet content based on functions such as Web addresses and Web address keywords. Up to 32 entries are supported in the Keyword list.

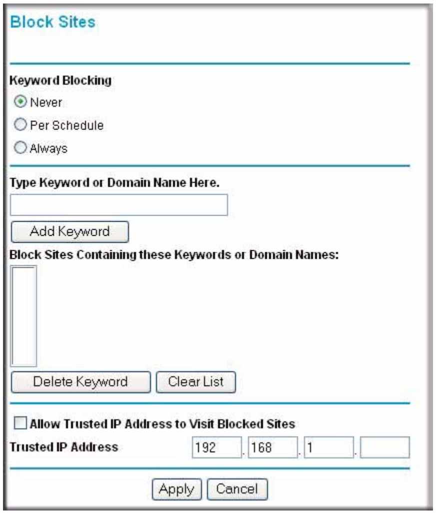
Table 3-1. Keyword Examples

Keyword	Description
XXX	The URL <http://www.badstuff.com/xxx.html> is blocked.
.com	Only websites with other domain suffixes (such as .edu or .gov) can be viewed.
.	This blocks all Internet browsing access.

Blocking a Keyword or Domain

To block a keyword or domain:

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. On the main menu, select **Block Sites** under Content Filtering. The Block Sites screen displays.



Block Sites

Keyword Blocking

● Never

○ Per Schedule

○ Always

Type Keyword or Domain Name Here.

Block Sites Containing these Keywords or Domain Names:

☐ Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address 192 . 168 . 1 .

Figure 3-1

3. To enable keyword blocking, select one of the following:
- **Per Schedule**. Block keywords according to the settings in the Schedule screen.
- **Always**. Turn on keyword blocking all the time, independent of settings in the Schedule screen.

4. Type a keyword or domain, click **Add Keyword**, and then click **Apply**.

Deleting Keywords or Domains

To delete a keyword or domain:

1. Select the keyword or domain from the list.

2. Click **Delete Keyword**, and then click **Apply**.

Trusted IP Address

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.

To specify a trusted user:

1. In the **Trusted IP Address** field, type the computer’s IP address.

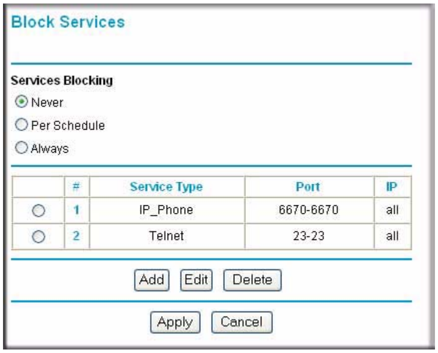
2. Click **Apply**.

Blocking Services

The router allows you to block the use of certain Internet services by PCs on your network. You can block specific services or filter by IP address or by a range of IP addresses. You can block these services all the time or set blocking for certain days and times.

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

Select **Block Services** under Content Filtering in the main menu. The Block Services screen displays.



Block Services

Services Blocking

● Never
○ Per Schedule
○ Always

	#	Service Type	Port	IP
○	1	IP_Phone	6670-6670	all
○	2	Telnet	23-23	all

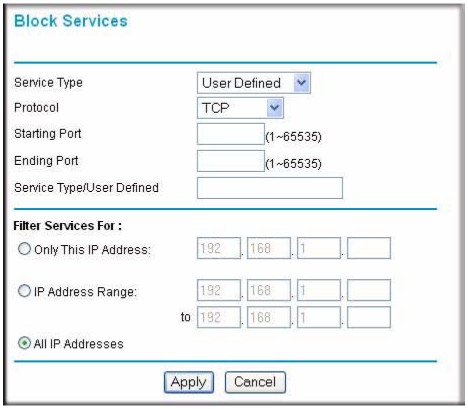
Figure 3-2

Blocking by Specific Service

To enable service blocking, select either **Per Schedule** or **Always**, then click **Apply**. If you want to block by schedule, be sure that a time period is specified in the Schedule screen (see "Schedule" on page 3-7).

To specify a service for blocking:

1. On the Block Services screen, click **Add**. The screen changes to display the setup options:



Block Services

Service Type	User Defined
Protocol	TCP
Starting Port	(1~65535)
Ending Port	(1~65535)
Service Type/User Defined	

Filter Services For :

○ Only This IP Address: 192 . 168 . 1 .

○ IP Address Range: 192 . 168 . 1 .
to 192 . 168 . 1 .

● All IP Addresses

Figure 3-3

2. From the **Service Type** list, select the application or service to be allowed or blocked. The list already displays several common services, and if you select one of them, the screen then displays the settings appropriate for that service.
   - As you add services to be blocked, after you click **Apply,** those services are included in the Service table (Figure 3-2 on page 3-5).
   - You are not limited to the choices predefined in the **Service Type** list. You can create custom services as described in the following section.

Adding Custom Services

To add any additional services or applications that are not in the Service Type list:

1. Select **User Defined** in the **Service Type** list.
2. Enter the name of the user-defined service or application in the **Service Type/User Defined** field (below **Ending Port**).
3. From the **Protocol** list, if you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **TCP/UDP**.
4. Enter the **Starting Port** and **Ending Port** numbers. If the application uses a single port number, enter that number in both fields.
5. Click **Apply**.

   The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, “Assigned Numbers.” Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups.

Blocking by Filtering IP Addresses

To block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network (Figure 3-3 on page 3-5):

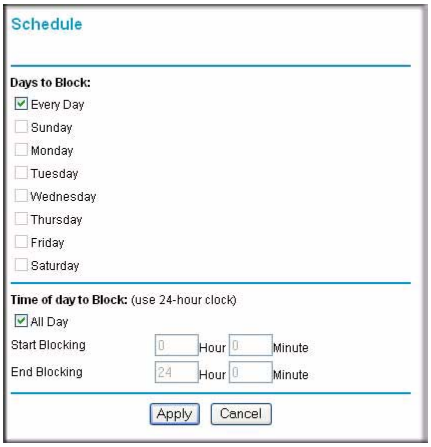
1. To filter by IP address, select one of the following under Filter Services For:
   - To block a single computer, select **Only This IP Address**, and enter that computer’s IP address.
   - To block a group of computers that have consecutive IP addresses, select **IP Address Range**, and enter the beginning and the end of the IP address range.
   - To block all computers, select **All IP Addresses**.

2. Click **Apply**.

Schedule

The router allows you to specify days and times when blocking (see “Blocking Sites” on page 3-2 and “Blocking Services” on page 3-4) is enforced.

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. From the main menu, select **Schedule** to display the following screen:



Schedule

Days to Block:

☑ Every Day
□ Sunday
□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday

Time of day to Block: (use 24-hour clock)

☑ All Day

Start Blocking 0 Hour 0 Minute
End Blocking 24 Hour 0 Minute

Figure 3-4

3. Enter the days and the time of day that you want to schedule:
   - Select **Every Day**, or select one or more days.
   - To limit access for the selected days, select the **All Day** check box.
   - To limit access during certain times on the selected days, type a start time and end time.
     – Enter the time in 24-hour time format. For example, to specify 10:30 a.m., enter 10 hours and 30 minutes. To enter 10:30 p.m., enter 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.

  – You can verify your time zone in the E-Mail screen (see "Enabling Security Event E-mail Notification" on page 4-9).

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

Chapter 4
Managing Your Network

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

Backing Up, Restoring, and Erasing Your Settings

The configuration settings of the wireless router are stored in a configuration file in the wireless router. This file can be backed up to your computer, restored, or erased to restore factory default settings. The following sections explain how to perform these tasks.

Backing Up the Configuration to a File

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. On the main menu, select **Backup Settings** under Maintenance.

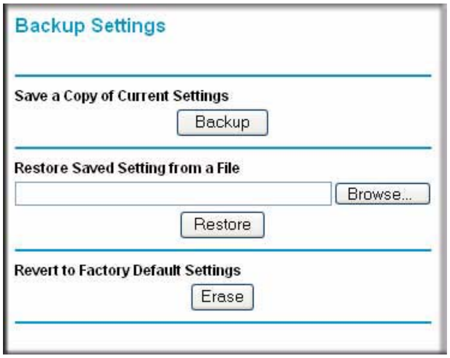

Backup Settings
Save a Copy of Current Settings
Backup
Restore Saved Setting from a File
Browse...
Restore
Revert to Factory Default Settings
Erase

Figure 4-1

3. To save a copy of the current settings, click **Backup**.
4. Store the .cfg file on a computer on your network.

Restoring the Configuration from a File

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. On the main menu, select **Backup Settings** under Maintenance.
3. Enter the full path to the file on your network, or click **Browse** to locate the file.
4. When you have located the .cfg file, click **Restore** to upload the file to the wireless router.
5. The wireless router reboots.

Erasing the Configuration

You can restore the wireless router to its factory default settings using the Erase function.

1. On the main menu, select **Backup Settings** under Maintenance.
2. Click **Erase**.
3. The wireless router reboots.

   After you erase settings, the wireless router password is **password**, the LAN IP address is **192.168.0.1**, and the wireless router DHCP client is enabled.

➡

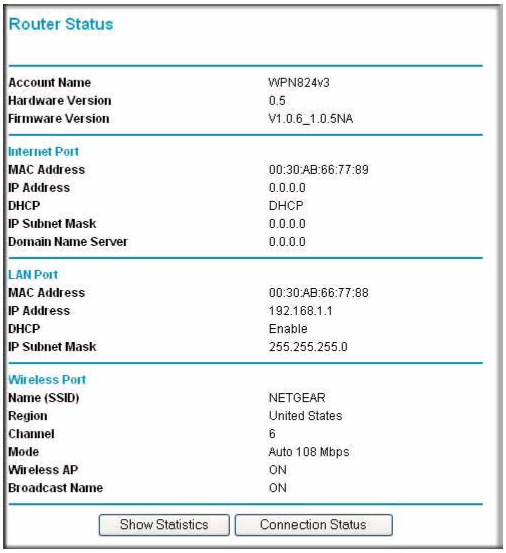
Network Management Information

The wireless router provides a variety of status and usage information:

- **Router status**. See “Viewing Wireless Router Status and Usage Statistics” on page 4-3.
- **Viewing attached devices**. See “Viewing Attached Devices” on page 4-7.
- **Logs**. See “Viewing, Selecting, and Saving Logged Information” on page 4-7.

Viewing Wireless Router Status and Usage Statistics

When you log in to the wireless router, the Router Status screen opens. You can also select **Router Status** under Maintenance on the main menu to view this screen.



Router Status

Account Name	WPN824v3
Hardware Version	0.5
Firmware Version	V1.0.6_1.0.5NA
Internet Port	
MAC Address	00:30:AB:66:77:89
IP Address	0.0.0.0
DHCP	DHCP
IP Subnet Mask	0.0.0.0
Domain Name Server	0.0.0.0
LAN Port	
MAC Address	00:30:AB:66:77:88
IP Address	192.168.1.1
DHCP	Enable
IP Subnet Mask	255.255.255.0
Wireless Port	
Name (SSID)	NETGEAR
Region	United States
Channel	6
Mode	Auto 108 Mbps
Wireless AP	ON
Broadcast Name	ON

Figure 4-2

The following table explains the Router Status fields.

Table 4-1. Router Status Fields

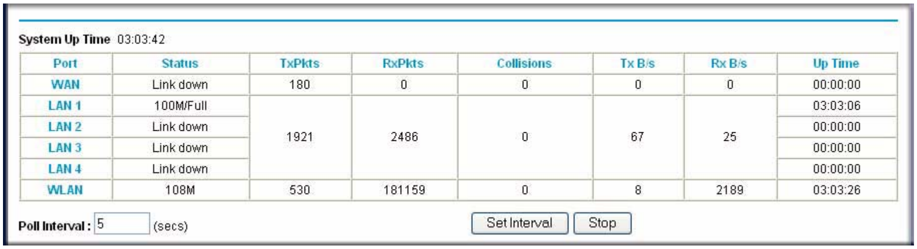
Field	Description
Account Name	The host name assigned to the wireless router in the Basic Settings screen.
Hardware Version	The wireless router hardware version.
Firmware Version	The wireless router firmware version.

Table 4-1. Router Status Fields (continued)

Field		Description
Internet Port	MAC Address	The Ethernet MAC address being used by the Internet (ADSL) port of the wireless router.
	IP Address	The IP address used by the Internet (ADSL) port of the wireless router. If no address is shown, the wireless router cannot connect to the Internet.
	DHCP	Indicates if the IP address is assigned automatically.
	IP Subnet Mask	The IP subnet mask used by the Internet (ADSL) port of the wireless router.
	Domain Name Server	The Domain Name Server (DNS) IP addresses used by the wireless router. These addresses are usually obtained dynamically from the ISP.
LAN Port	MAC Address	The Ethernet MAC address used by the local (LAN) port of the wireless router.
	IP Address	The IP address used by the local (LAN) port of the wireless router. The default is 168.192.0.1.
	DHCP	• If Off, the wireless router does not assign IP addresses to PCs on the LAN. • If On, the wireless router assigns IP addresses to PCs on the LAN.
	IP Subnet Mask	The IP subnet mask used by the local (LAN) port of the wireless router. The default is 255.255.255.0.
Wireless Port. See Chapter 2, "Wireless Settings," for details.	Name (SSID)	The service set ID, also known as the wireless network name.
	Region	The country where the unit is set up for use.
	Channel	The current channel, which determines the operating frequency.
	Mode	The current wireless connection mode.
	Wireless AP	Indicates if the Access Point feature is disabled or not. If not enabled, the Wireless light on the front panel turns off.
	Broadcast Name	Indicates if the wireless router is configured to broadcast its SSID.

Statistics

To view statistics, click **Show Statistics** to display the following screen:



System Up Time 03:03:42

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Link down	180	0	0	0	0	00:00:00
LAN 1	100M/Full	1921	2486	0	67	25	03:03:06
LAN 2	Link down						00:00:00
LAN 3	Link down						00:00:00
LAN 4	Link down						00:00:00
WLAN	108M	530	181159	0	8	2189	03:03:26

Poll Interval : 5 (secs)

Figure 4-3

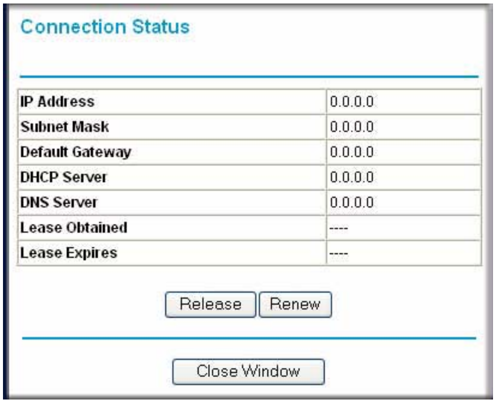
The following table explains the Router Statistics screen fields.

Table 4-2. Router Statistics Fields

	Description
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.
Poll Interval	Specifies the interval at which the statistics are updated in this window. To freeze the display, click **Stop**.

Connection Status

To view the connection status, click **Connection Status** on the Router Status screen. The Connection Status screen displays:



Connection Status

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DHCP Server	0.0.0.0
DNS Server	0.0.0.0
Lease Obtained	----
Lease Expires	----

Figure 4-4

The following table describes the fields in the Connection Status screen:

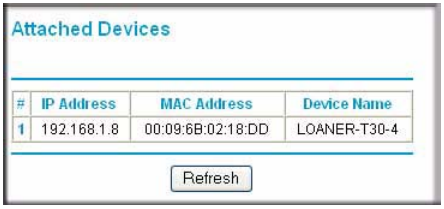
Table 4-3. Connection Status Fields

Field	Description
IP Address	The IP address assigned to the WAN port by the Internet service provider.
Subnet Mask	The WAN (Internet) subnet mask assigned to the router.
Default Gateway	The WAN (Internet) default gateway that the router communicates with.
DHCP Server	Indicates either the client (IP address is obtained dynamically) or none.
DNS Server	The IP address of the Domain Name Service (DNS) server that provides translation of network names to IP addresses.
Lease Obtained	The start time for the wireless router IP address provided by the Internet Service Provider.
Lease Expires	When the lease expires, the wireless router can ask the Internet Service Provider to renew the IP address.

Viewing Attached Devices

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

From the main menu, select **Attached Devices**:



Attached Devices

#	IP Address	MAC Address	Device Name
1	192.168.1.8	00:09:6B:02:18:DD	LOANER-T30-4

Figure 4-5

For each device, the table shows the IP address, device name if available, and the Ethernet MAC address.

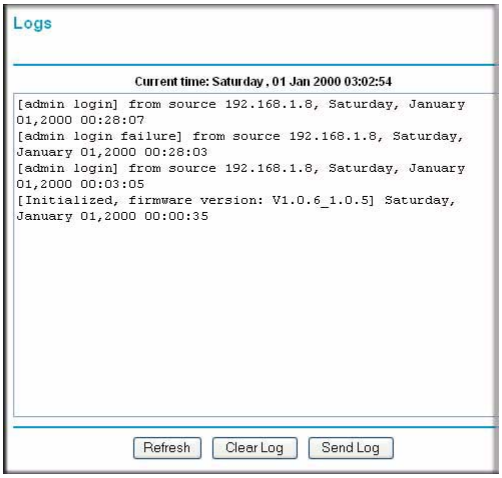
➡	

To force the wireless router to look for attached devices, click **Refresh**.

Viewing, Selecting, and Saving Logged Information

The wireless router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites screen, the Logs screen can show you when someone on your network tries to access a blocked site. If you enabled e-mail notification, you receive these logs in an e-mail message. If you do not have e-mail notification enabled, you can view the logs here.

An example of the logs file is shown in the following figure:



Logs

Current time: Saturday , 01 Jan 2000 03:02:54

```
[admin login] from source 192.168.1.8, Saturday, January
01,2000 00:28:07
[admin login failure] from source 192.168.1.8, Saturday,
January 01,2000 00:28:03
[admin login] from source 192.168.1.8, Saturday, January
01,2000 00:03:05
[Initialized, firmware version: V1.0.6_1.0.5] Saturday,
January 01,2000 00:00:35
```

Figure 4-6

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, 2002-05-21 18:48:39 - NETGEAR activated
```

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

```
Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:10.1.1.2
Thu, 2002-05-21 18:56:58 - Administrator logout - IP:10.1.1.2
```

[This entry shows an administrator logging in to and out from IP address 10.1.1.2.]

```
Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:10.1.1.2
```

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

```
Wed, 2002-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was e-mailed.]

Dropped Packets

```
Wed, 2002-05-22 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, 2002-05-22 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, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

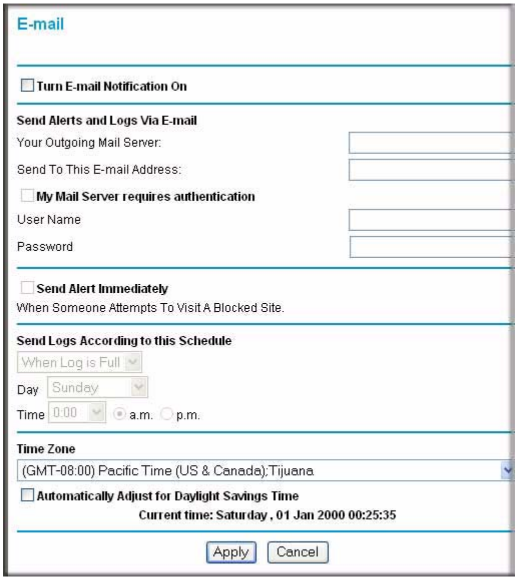
These entries show an inbound FTP (port 21) packet, User Datagram Protocol (UDP) packet (port 6970), and Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.

Enabling Security Event E-mail Notification

To receive logs and alerts by e-mail, you must enter your e-mail information in the E-mail screen.

To enable e-mail notification:

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. Under Content Filtering in the main menu, select **E-mail**:



E-mail

□ Turn E-mail Notification On

Send Alerts and Logs Via 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

When Log is Full

Day Sunday

Time 0:00 ● a.m. ○ p.m.

Time Zone

(GMT-08:00) Pacific Time (US & Canada);Tijuana

□ Automatically Adjust for Daylight Savings Time

Current time: Saturday , 01 Jan 2000 00:25:35

Figure 4-7

3. Enter the settings for this screen.

- **Turn E-mail Notification On**. Select this check box if you want to receive e-mail logs and alerts from the wireless router.
- **Send Alerts and Logs Via E-mail**.
  - **Send To This E-mail Address**. Enter the e-mail address where you want to send the alerts and logs. Use a full e-mail address, such as ChrisXY@myISP.com.
  - **Outgoing Mail Server**. Enter the name or IP address of the outgoing SMTP mail server of your ISP (such as mail.myISP.com).
  - **My Mail Server requires authentication**. Select this check box if you need to log in to your SMTP server to send e-mail. If you select this check box, you must enter the user name and password for the mail server.
- **Send Alert 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 or daily.
  - **Time for sending log**. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

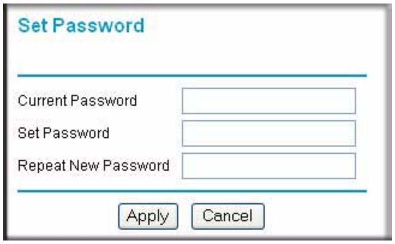
If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the wireless router’s memory. If the wireless router cannot e-mail the log file, the log buffer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

Setting the Password

The Set Password screen allows you to change the default password for the wireless router, **password**, to a more secure password. (For more information about logging in and the default settings, see “Using Automatic Firmware Update upon Login” on page 1-3 and “Restoring the Default Settings” on page A-3.)

To change the password:

1. Select **Set Password** under Maintenance in the main menu. The Set Password screen displays:



Set Password

Current Password

Set Password

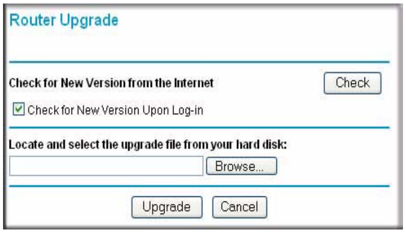
Repeat New Password

Figure 4-8

2. Enter the current password, then enter the new password twice.
3. Click **Apply**.

Router Upgrade

The Router Upgrade screen allows you to manage firmware updates after you have installed your wireless router. Select **Router Upgrade** under Maintenance in the main menu. The Router Upgrade screen displays:



Router Upgrade

Check for New Version from the Internet [Check]

☑ Check for New Version Upon Log-in

Locate and select the upgrade file from your hard disk:

[Browse...]

[Upgrade] [Cancel]

Figure 4-9

The following options are available:

- **Check for New Version from the Internet**. The wireless router checks the NETGEAR database for a newer firmware image file and compares it to your currently installed version. To force the router to check for a newer version, click **Check**.
  - If a new version is found, you are asked about upgrading. Click **Yes** to update your firmware.

    ⚠

  - If no new firmware version is available, the message **No New Firmware Version Available** displays.
- **Check for New Version Upon Login**. If this option is selected (the default), the router checks the NETGEAR database for a newer firmware image file every time you log in. To disable this feature, clear the check box.
- **Locate and select the upgrade file from your hard disk**. Use this field, and the **Browse** and **Upgrade** buttons, to manually check for new firmware.

Manually Checking for New Firmware

To manually check and upload new firmware:

➡

1. Log in to the wireless router.
2. Select **Wireless Extender Status** on the main menu. When the Wireless Extender Status screen displays, note the version number of your router firmware.
3. Go to *http://www.NETGEAR.com/support*, and select **Downloads** from the menu bar.
4. From the **Product Selection** drop-down list, select **WPN824v3**. The Product Support page for your router displays.
5. Under Downloads**,** check the most recent firmware version offered against the firmware version shown on your Wireless Extender Status screen.
6. If the version on the NETGEAR website is more recent, click the version number. Then, click **Right-click and Save to Download**, and save the file to a location on your hard disk.

Manually Upgrading Firmware

After you have downloaded firmware as described in the previous section, follow these steps to upgrade your wireless router:

1. Log in to the wireless router.
2. Select **Firmware Update** under Maintenance in the main menu.
3. Click **Browse** and locate the unzipped firmware image that you downloaded to your PC (the file ends in .img or .chk).
4. Once you have selected the file, click **Upload** to send the software to the router. The upload process takes several minutes. When the software upload process is complete, the router restarts.

⚠

5. After the router has restarted, select **Wireless Router Status** under Management in the main menu. Check the firmware version to verify that your router now has the new software installed.

6. Click **Browse** to locate the binary (.bin or .img) upgrade file, and then click **Upload**.

⚠	

Chapter 5
Advanced Settings and Features

This chapter describes features available under Advanced in the main menu of your wireless router.

Wireless Repeating (Also Called WDS)

The wireless router can be used with a wireless access point (AP) to build large bridged wireless networks. Wireless repeating is a type of Wireless Distribution System (WDS).

The following figure shows a wireless repeating scenario:

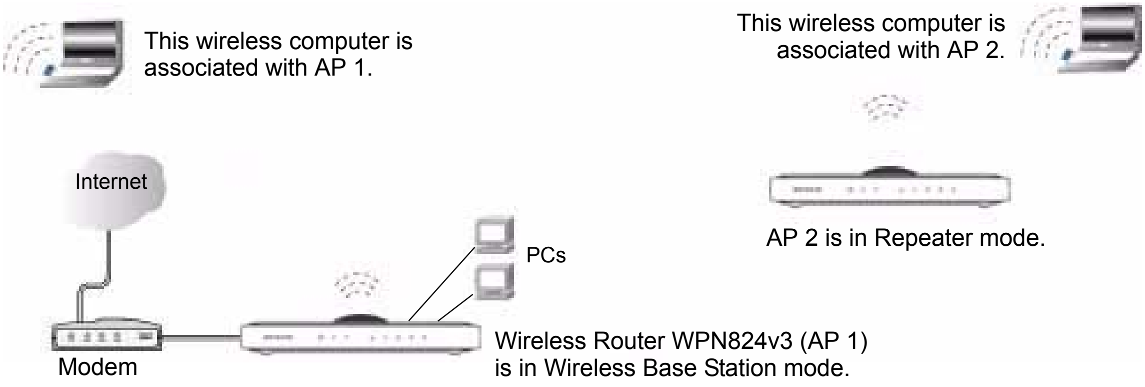

This wireless computer is associated with AP 1.
This wireless computer is associated with AP 2.
Internet
PCs
AP 2 is in Repeater mode.
Modem
Wireless Router WPN824v3 (AP 1) is in Wireless Base Station mode.

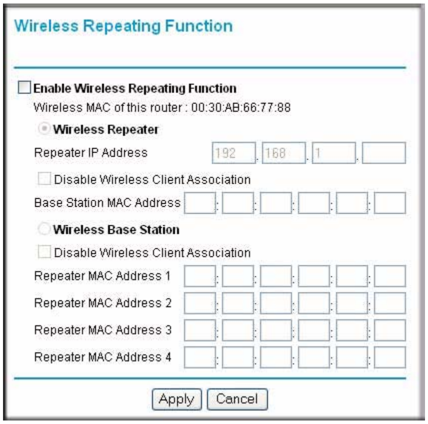
Figure 5-1

In the scenario shown, the following conditions must be met for both APs:

- Both APs must use the same SSID, wireless channel, authentication mode (if any), and encryption mode (see information about WEP in "Configuring WEP" on page 2-9).
- Both APs must be on the same LAN IP subnet. That is, all the AP LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) must be configured to operate in the same LAN network address range as the APs.
- If you are using DHCP, the **Get Dynamically From ISP Gateway** radio button in the Internet IP Address section of the Basic Settings screen should be selected for all AP devices in the IP Address Source section.

Wireless Repeating Function Screen

You can view or change wireless repeater settings for the wireless router. Select **Wireless Repeating Function** under Advanced in the main menu of the router to display the following screen:



Wireless Repeating Function

□ Enable Wireless Repeating Function

Wireless MAC of this router : 00:30:AB:66:77:88

● Wireless Repeater

Repeater IP Address 192 . 168 . 1 .

□ 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 : : : : :

Figure 5-2

The wireless router supports two modes of the wireless repeating function, and allows you to control wireless client association:

- **Wireless Base Station mode**. The wireless router acts as the parent AP, bridging traffic to and from the child repeater AP, as well as handling wireless and wired local computers. To configure this mode, you must know the MAC addresses of the child repeater AP.

- **Wireless Repeater mode**. The wireless router sends all traffic from its local wireless or wired computers to a remote AP. To configure this mode, you must know the MAC address of the remote parent AP.
- **Disable Wireless Client Association**. Usually this check box is cleared so that the router is an access point for wireless computers.

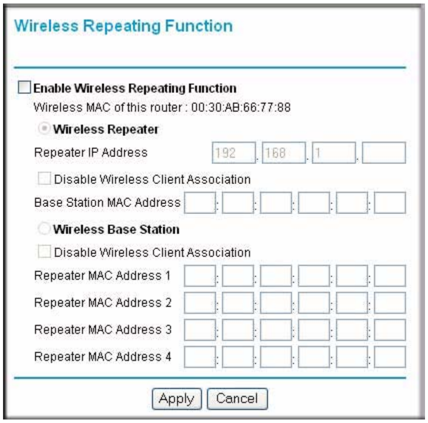
  If this check box is selected, the router communicates wirelessly only with other APs whose MAC addresses are listed in this screen. The router still communicates with wire-connected LAN devices.

Setting Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy chained. You must know the wireless settings for both units. You must know the MAC address of the remote unit. First, set up the base station, and then set up the repeater.

To set up the base station:

1. Set up both units with exactly the same wireless settings (SSID, mode, channel, and security). Note that the wireless security option must be set to WEP or None.
2. On the wireless router base unit, select **Wireless Repeating Function** under Advanced in the main menu of the router. The Wireless Repeating Function screen displays.



Wireless Repeating Function

□ Enable Wireless Repeating Function

Wireless MAC of this router : 00:30:AB:66:77:88

○ Wireless Repeater

Repeater IP Address 192 . 168 . 1 .

□ 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 : : : : :

Figure 5-3

3. Select the **Enable Wireless Repeating Function** check box and the **Wireless Base Station** radio button.

4. Enter the MAC address for the repeater units.
5. Click **Apply** to save your changes.

Setting Up a Repeater Unit

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

To configure a Wireless Router Model WPN824v3 as a repeater unit:

1. If you are using the same model of wireless router for both the base station and repeaters, then you must change the LAN IP address for each repeater to a different IP address in the same subnet (see "Specifying LAN IP Settings" on page 5-7).
2. Check the Wireless Settings screen, and verify that the wireless settings match the base unit exactly. The wireless security option must be set to WEP or None.
3. On the Wireless Repeating Function screen, select the **Enable Wireless Repeating Function** check box.

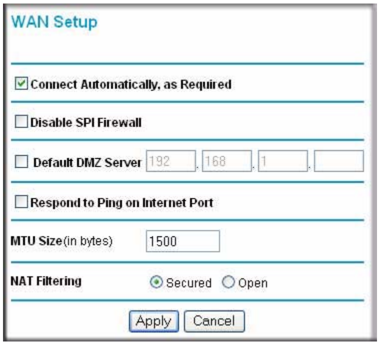
   In the **Repeater IP Address field**, the router's IP address is automatically filled in. This IP address must be in the same subnet as the base station but different from the LAN IP of the base station.
4. Fill in the **Base Station MAC Address** field.
5. Click **Apply** to save your changes.
6. Verify connectivity across the LANs.

   A computer on any wireless or wired LAN segment of the wireless router should be able to connect to the Internet or share files and printers with any other wireless or wired computer or server connected to the other AP.

Viewing or Changing WAN Settings

To view or change settings on the WAN Setup screen:

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. From the main menu, select **WAN Setup**. The WAN Setup screen displays:



WAN Setup

☑ Connect Automatically, as Required

□ Disable SPI Firewall

□ Default DMZ Server 192 . 168 . 1 .

□ Respond to Ping on Internet Port

MTU Size(in bytes) 1500

NAT Filtering ● Secured ○ Open

Figure 5-4

The following table explains the settings in the WAN Setup screen:

Table 5-1. WAN Setup Screen Settings

Setting	Description
Connect Automatically, as Required	• Normally, this option should be selected, so that an Internet connection is made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can clear this check box. • If the check box is not selected, you must connect manually. To do this, click the **Connection Status** button on the Status screen. • If you have an "Always on" connection, this setting has no effect.
Disable SPI Firewall	The firewall protects your LAN against port scans and denial of service (DoS) attacks. This check box should be cleared only in special circumstances.
Default DMZ Server	The Default DMZ Server feature is helpful when you use some online games and videoconferencing applications that are incompatible with NAT. Note that this feature reduces the effectiveness of the firewall. For more information, see "Setting Up a Default DMZ Server" on page 5-6.

Table 5-1. WAN Setup Screen Settings (continued)

Setting	Description
Respond to Ping on Internet WAN Port	If you want the wireless router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, since it allows your wireless 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 Transmission 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 that it is necessary for your ISP connection.
NAT Filtering	The wireless router uses Network Address Translation (NAT), so your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers.

Setting Up a Default DMZ Server

The Default DMZ Server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with NAT. The wireless 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.

⚠

Usually the wireless router discards incoming traffic from the Internet unless it is a response to a local computer or a service that is configured in the Ports screen. Instead of discarding this traffic, you can forward it to a computer on your network. This computer is the default DMZ server.

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

1. Log in to the wireless router (see "Logging In to the Wireless Router" on page 1-2).
2. From the main menu, select **WAN Setup** under the Advanced heading.
3. Select the **Default DMZ Server** check box, and type the IP address for that server.
4. Click **Apply** to save your changes.

Specifying LAN IP Settings

You can use the LAN IP Setup screen to view or change the settings for LAN IP services such as DHCP and RIP. The wireless router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The wireless router default LAN IP configuration is:

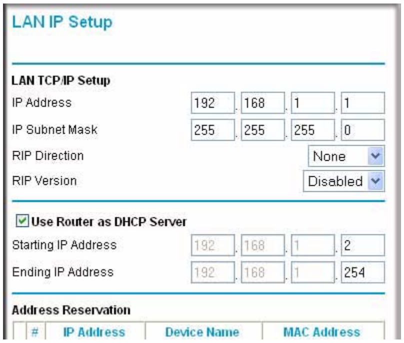
- LAN IP addresses. 192.168.1.1
- Subnet mask. 255.255.255.0

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.

To view or change the LAN IP settings:

⚠

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. From the main menu, select **LAN IP Setup** to display the following screen:



LAN IP Setup

LAN TCP/IP Setup

IP Address 192 . 168 . 1 . 1

IP Subnet Mask 255 . 255 . 255 . 0

RIP Direction None

RIP Version Disabled

☑ Use Router as DHCP Server

Starting IP Address 192 . 168 . 1 . 2

Ending IP Address 192 . 168 . 1 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

Figure 5-5

The following table explains the settings on the LAN IP Setup screen.

Table 5-2. LAN IP Setup Screen Settings

	Description
IP Address	The LAN IP address of the wireless router.
IP Subnet Mask	The LAN subnet mask of the wireless 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 router.
RIP Direction	RIP (Router Information Protocol) allows a wireless router to exchange routing information with other routers. The RIP Direction selection controls how the wireless router sends and receives RIP packets. • **Both**. The wireless router broadcasts its routing table periodically, and it incorporates the RIP information that it receives. • **Out Only**. The wireless router broadcasts its routing table periodically, but ignores any RIP packets received. • **In Only**. The wireless router incorporates the RIP information that it receives, but it does not broadcast its routing table. • **None**. The wireless router does not send any RIP packets and ignores any RIP packets received.
RIP Version	This controls the format and the broadcasting method of the RIP packets that the wireless router sends. It recognizes both formats when receiving. By default, this is set to RIP-1. • **RIP-1** is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup. • **RIP-2** carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. • **RIP-2B** uses subnet broadcasting. • **RIP-2M** uses multicasting.
Access Router Management Interface on additional port	This option is available only if you have disabled Network Address Translation and you have been assigned a fixed address by your ISP. This allows your router to be managed remotely on a specially assigned port instead of the HTTP port (80).
Use Router as DHCP Server	By default, the wireless 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 router's LAN. See "Using the Router as DHCP Server."
Address Reservation	Specify a reserved IP address for a computer on the LAN, so that it always receives the same IP address when it access the router's DHCP server. See "Reserved IP Addresses."

DHCP Server

By default, the wireless 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 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 the LAN IP Setup 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. For an explanation of DHCP and help with assigning IP addresses, click the link to the online document “TCP/IP Networking Basics” in Appendix B.

Using the 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 filling in the **Starting IP Address** and **Ending IP Address** fields. 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 192.168.1.2 and 192.168.1.100, although you might want to save part of the range for devices with fixed addresses.

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

- An IP address from the range you have defined.
- Subnet mask.
- Gateway IP address; 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 addresses of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server’s IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

Reserved IP Addresses

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address when 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. Log in to the wireless router (see “Logging In to the Wireless Router” on page 1-2, and select **LAN IP Setup**.
2. In the Address Reservation section on the LAN IP Setup screen, click **Add**.
3. In the **IP Address field**, type the IP address to assign to the computer or server. Choose an IP address from the router’s LAN subnet, such as 10.1.1.x.
4. Type the MAC address of the computer or server.

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

To edit or delete a reserved address entry:

1. In the Address Reservation table on the LAN IP Setup screen, select the radio button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

Configuring Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your

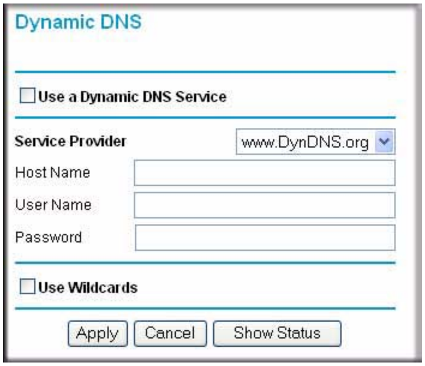
IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service that will allow you to register your domain to their IP address and will forward traffic directed at your domain to your frequently changing IP address.

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

To configure Dynamic DNS:

⚠	

1. Log in to the wireless router (see "Logging In to the Wireless Router" on page 1-2).
2. From the main menu, select **Dynamic DNS**. The Dynamic DNS screen displays:



Dynamic DNS

□ Use a Dynamic DNS Service

Service Provider	www.DynDNS.org
Host Name	
User Name	
Password	

□ Use Wildcards

Figure 5-6

3. Access the website of one of the Dynamic DNS service providers whose names are in the **Service Provider** drop-down list, and register for an account.

   For example, for dyndns.org, go to www.dyndns.org.

4. Select the **Use a Dynamic DNS Service** check box.
5. From the **Service Provider** drop-down list, select the name of your Dynamic DNS service provider.

6. In the **Host Name** field, type the host name that your Dynamic DNS service provider gave you.

7. Type the user name and 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.

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 10.1.1.100.
- Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the wireless router, and a second static route was created to your local network for all 10.1.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 10.1.1.100. The static route would look like Figure 5-7.

In this example:

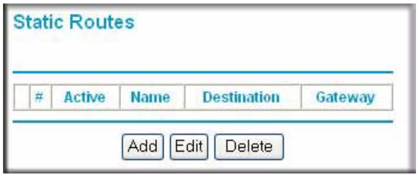
- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Wireless Router IP Address** field specifies that all traffic for these addresses should be forwarded to the ISDN router at 10.1.1.100.
- A **Metric** value of 1 works because the ISDN router is on the LAN.
  This represents the number of routers between your network and the destination. This is a direct connection, so it is set to 1.
- **Private** is selected only as a precautionary security measure in case RIP is activated.

Configuring Static Routes

You can add static routes, and view or change existing static routes from the Static Routes screen.

To add or edit a static route:

1. Log in to the wireless 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 router.
2. On the main menu, select **Static Routes** under Advanced. The Static Routes screen displays:



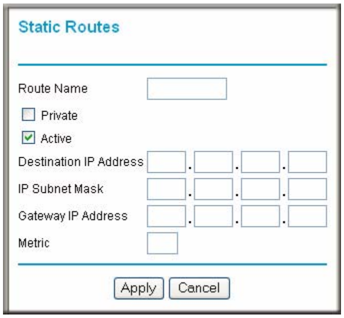
Static Routes

	#	Active	Name	Destination	Gateway

Figure 5-7

Existing static routes are shown in the Static Routes table.

3. Click **Add** or **Edit.** The following screen displays:



Static Routes

Route Name

□ Private

☑ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

Figure 5-8

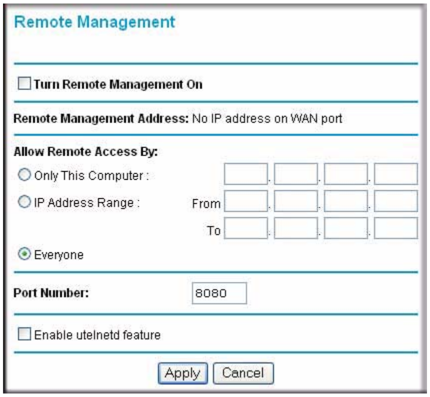
4. Enter the settings for the static route.
   - **Route Name**. This is for identification purposes only.
   - **Private**. If you want to limit access to the LAN only, then select this check box. The static route will not be reported in RIP.
   - **Active**. You must select this check box to make this route effective.
   - **Destination IP Address**. The IP address of the final destination.
   - **IP Subnet Mask**. If the destination is a single host, type **255.255.255.255**.
   - **Gateway IP Address**. This must be a router on the same LAN segment as your wireless router.
   - **Metric**. Type a number between 2 and 15. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 2.
5. Click **Apply**. The static route is added to the Static Routes table.

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 router.

To configure remote management:

1. Log in to the wireless router at its default LAN address of **http://192.168.1.1** 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 router.
2. On the main menu, select **Remote Management** under Advanced. The Remote Management screen displays:



Remote Management

☐ Turn Remote Management On

Remote Management Address: No IP address on WAN port

Allow Remote Access By:

○ Only This Computer :

○ IP Address Range : From . . .

To . . .

● Everyone

Port Number: 8080

☐ Enable utelnetd feature

Figure 5-9

3. Select the **Turn Remote Management On** check box.
4. Specify which external addresses will be allowed to access the wireless 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.

5. Type 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.

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

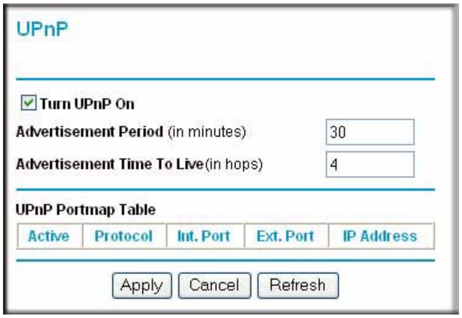
   When accessing your wireless router from the Internet, you will type your wireless router's WAN IP address in your browser's Address (in IE) or Location (in Netscape) field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter in your browser:

   http://134.177.0.123:8080

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.

1. On the main menu, select **UPnP**. The UPnP screen displays:



UPnP

☑ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time To Live (in hops) 4

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

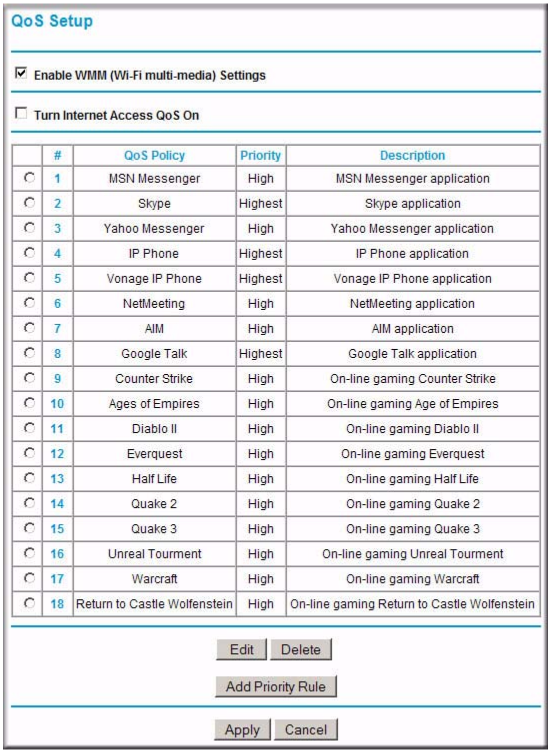
Figure 5-10

2. Fill in the fields in the UPnP screen:
   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. This check box is selected by default. If you clear this check box, the wireless router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the wireless router.
   - **Advertisement Period**. The advertisement period is how often the wireless 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 (in hops)**. 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 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. Click **Apply** to save your changes.

   To update the Portmap Table to show the active ports that are currently opened by UPnP devices, click **Refresh**.

QoS Setup

QoS is an advanced feature that you can use to prioritize some types of traffic ahead of others. The wireless router can provide QoS prioritization over the wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen. Select **QoS Setup** under Advanced in the main menu. The QoS Setup screen displays:



QoS Setup

☑ Enable WMM (Wi-Fi multi-media) Settings

☐ Turn Internet Access QoS On

	#	QoS Policy	Priority	Description
○	1	MSN Messenger	High	MSN Messenger application
○	2	Skype	Highest	Skype application
○	3	Yahoo Messenger	High	Yahoo Messenger application
○	4	IP Phone	Highest	IP Phone application
○	5	Vonage IP Phone	Highest	Vonage IP Phone application
○	6	NetMeeting	High	NetMeeting application
○	7	AIM	High	AIM application
○	8	Google Talk	Highest	Google Talk application
○	9	Counter Strike	High	On-line gaming Counter Strike
○	10	Ages of Empires	High	On-line gaming Age of Empires
○	11	Diablo II	High	On-line gaming Diablo II
○	12	Everquest	High	On-line gaming Everquest
○	13	Half Life	High	On-line gaming Half Life
○	14	Quake 2	High	On-line gaming Quake 2
○	15	Quake 3	High	On-line gaming Quake 3
○	16	Unreal Tourment	High	On-line gaming Unreal Tourment
○	17	Warcraft	High	On-line gaming Warcraft
○	18	Return to Castle Wolfenstein	High	On-line gaming Return to Castle Wolfenstein

Figure 5-11

Using WMM QoS for Wireless Multimedia Applications

The wireless router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS is a feature that 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, WMM must be enabled for both the wireless router and the client running the application. 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.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen, shown in Figure 5-11 on page 5-18, by clearing the **Enable WMM** check box and clicking **Apply**.

Configuring QoS for Internet Access

You can give prioritized Internet access to the following types of traffic:

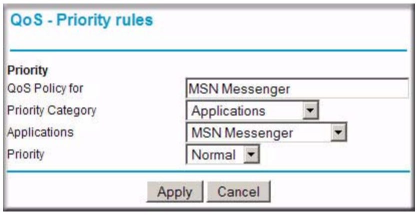
- For specific applications
- For specific online games
- On individual Ethernet LAN ports of the router
- From a specific device by MAC address.

To specify prioritization of traffic, you must create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

QoS for Applications and Online Gaming

To create a QoS policy for applications and online games:

1. Select **QoS Setup** under Advanced in the main menu. The QoS Setup screen displays, shown in Figure 5-11 on page 5-18.
2. Click **Add Priority Rule**. The QoS - Priority Rules screen displays.



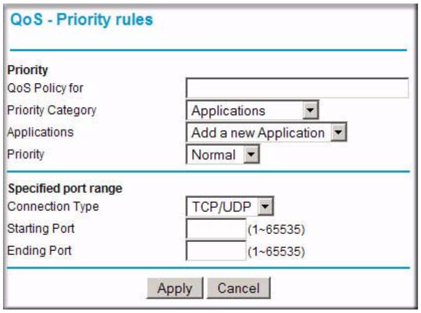
QoS - Priority rules

Priority

QoS Policy for	MSN Messenger
Priority Category	Applications
Applications	MSN Messenger
Priority	Normal

Figure 5-12

3. In the **Priority Category** list, select either **Applications** or **Online Gaming**. In either case, a list of predefined applications or games displays in the **Applications** drop-down list.
4. From the **Applications** drop-down list, you can select an existing item, or you can scroll to the bottom of the list and select **Add a New Application** or **Add a New Game**.
   a. If you chose to add a new entry, the screen expands as shown:



QoS - Priority rules

Priority
QoS Policy for
Priority Category: Applications
Applications: Add a new Application
Priority: Normal

Specified port range
Connection Type: TCP/UDP
Starting Port (1~65535)
Ending Port (1~65535)

Figure 5-13

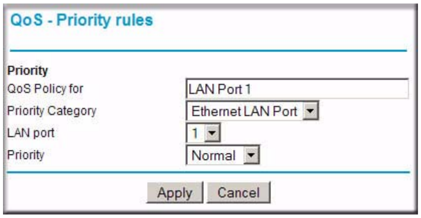
   b. In the **QoS Policy for** field, enter a descriptive name for the new application or game.
   c. Select the packet type, either **TCP** or **UDP** or both **(TCP/UDP)**, and specify the port number or range of port numbers used by the application or game.
5. From the **Priority** drop-down list, select the priority that this traffic should receive relative to other applications and traffic when accessing the Internet. The options are **Low**, **Normal**, **High**, and **Highest**.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
8. Click **Apply**.

QoS for a Router LAN Port

To create a QoS policy for a device connected to one of the router’s LAN ports:

1. Open the QoS Setup screen, shown in Figure 5-11 on page 5-18.
2. Click **Add Priority Rule**.

3. In the **Priority Category** list, select **Ethernet LAN Port**. The QoS Priority Rules screen changes:



QoS - Priority rules

Priority

QoS Policy for	LAN Port 1
Priority Category	Ethernet LAN Port
LAN port	1
Priority	Normal

Figure 5-14

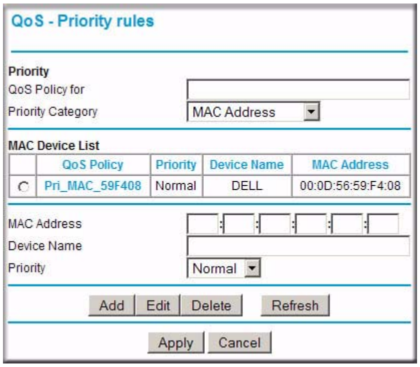
4. From the **LAN port** list, select the LAN port that will have a QoS policy.
5. From the **Priority** drop-down list, select the priority that this port's traffic should receive relative to other applications and traffic when accessing the Internet. The options are **Low**, **Normal**, **High**, and **Highest**.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box, and then click **Apply**.

QoS for a MAC Address

To create a QoS policy for traffic from a specific MAC address:

1. Open the QoS Setup screen, shown in Figure 5-11 on page 5-18.
2. Click **Add Priority Rule**.

3. In the **Priority Category** list, select **MAC Address**. The QoS Priority Rules screen changes:



QoS - Priority rules

Priority

QoS Policy for

Priority Category: MAC Address

MAC Device List

	QoS Policy	Priority	Device Name	MAC Address
○	Pri_MAC_59F408	Normal	DELL	00:0D:56:59:F4:08

MAC Address: : : : : :

Device Name

Priority: Normal

Figure 5-15

4. If the device to be prioritized is in the MAC Device List, select it. The information from the MAC Device List is used to populate the policy name, MAC Address, and Device Name fields. If the device is not in the MAC Device List, click **Refresh**. If it is still not there, you must complete these fields manually.
5. From the **Priority** drop-down list, select the priority that this device's traffic should receive relative to other applications and traffic when accessing the Internet. The options are **Low**, **Normal**, **High**, and **Highest**.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box, and then click **Apply**.

Editing or Deleting an Existing QoS Policy

To edit or delete an existing QoS policy:

1. Open the QoS Setup screen, shown in Figure 5-11 on page 5-18.
2. Select the radio button next to the QoS policy to be edited or deleted.
3. Do either of the following:
   - Click **Delete** to remove the QoS policy.
   - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.
4. Click **Apply** in the QoS Setup screen to save your changes.

Chapter 6
Troubleshooting

This chapter gives information about troubleshooting your Wireless Router Model WPN824v3. After each problem description, instructions are provided to help you diagnose and solve the problem.

Troubleshooting Quick Tips

This section describes tips for troubleshooting some common problems:

Be sure to restart your network in this sequence.

1. Turn off *and* unplug the modem.
2. Turn off the wireless router and computers.
3. Plug in the modem and turn it on. Wait 2 minutes.
4. Turn on the wireless router and wait 1 minute.
5. Turn on the computers.

Make sure that the Ethernet cables are securely plugged in.

- The Internet status light on the wireless router is lit if the Ethernet cable connecting the wireless router and the modem is plugged in securely and the modem and wireless router are turned on.
- For each powered-on computer connected to the wireless router by an Ethernet cable, the corresponding numbered router LAN port light is lit.

Make sure that the wireless settings in the computer and router match exactly.

- For a wirelessly connected computer, the wireless network name (SSID) and WEP or WPA security settings of the router and wireless computer must match exactly.
- If you have enabled the wireless router to restrict wireless access by MAC address, you must add the wireless computer’s MAC address to the router’s wireless card access list.

Make sure that the network settings of the computer are correct.

- Wired and wirelessly connected computers *must* have network (IP) addresses on the same network as the router. The simplest way to do this is to configure each computer to obtain an IP address automatically using DHCP. Click the link to the online document "Preparing Your Network" in Appendix B or the documentation that came with your computer.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. Your wireless router can capture and use that MAC address, as described in "Basic Settings for Your Internet Connection" on page 1-6.

Check the Test light to verify correct router operation.

If the Test light does not turn off within 2 minutes after you turn the router on, reset the router according to the instructions in "Restoring the Default Configuration and Password" on page 6-8.

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 light ⏻ is on.

2. After approximately 10 seconds, verify the following:

   a. The Power light is solid green.

   b. The LAN port lights are lit for any local ports that are connected.

   c. The Internet port light is lit.

   d. A port light is lit, to indicate that 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 light is green. If the port is 10 Mbps, the light is amber.

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

Power Light Is Not On

If the Power and other lights 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 correctly connected to a functioning power outlet.
- Check that you are using the 12V DC 1A power adapter supplied by NETGEAR for this product.

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

Lights Never Turn Off

When the router is turned on, the lights turn on for about 10 seconds and then turn off. If all the lights stay on, there is a fault within the router.

If all lights are still on one minute after power-up:

- Turn the power off and on to see if the router recovers.
- Clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.1.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 6-8.

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

LAN or Internet Port Lights Are Not On

If either the LAN lights or Internet light 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 that you are using the correct cable.
  When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Cannot Access the Router Main Menu

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

- 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 192.168.1.2 to 192.168.1.254. For instructions, click the link to the online document “Preparing Your Network” in Appendix B for information about how to configure your computer.

- If your router’s IP address has been 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 192.168.1.1. This procedure is explained in “Restoring the Default Configuration and Password” on page 6-8.
- 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 that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

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

- When entering configuration settings, be sure to click the **Apply** button before moving to another 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 first determine whether the router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser, and select an external site such as www.netgear.com.
2. Access the main menu of the router's configuration at *http://www.routerlogin.net*.
3. Under Maintenance, select **Router Status**.
4. Check that an IP address is shown for the WAN port.
   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

If your router is unable to obtain an IP address from the ISP, you might need to force your cable or DSL modem to recognize your new router by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your router.
3. Wait 5 minutes, and reapply power to the cable or DSL modem.
4. When the modem's lights indicate that it has reacquired sync with the ISP, reapply power to your router.
5. Then restart your computer.

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

- Your ISP might require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, the login name and password might be set incorrectly.
- Your ISP might check for your computer's host name.
  Assign the computer host name of your ISP account as the account name in the Basic Settings screen.

- 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 use your computer's MAC address. This can be done in the Basic Settings screen. See "Basic Settings for Your Internet Connection" on page 1-6.

If your 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 router's configuration, reboot your computer and verify the DNS address. For more information, click the link to the online document "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 router configured as its TCP/IP gateway.

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

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 or workstation.

Testing the LAN Path to Your Router

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

To ping the router from a 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 192.168.1.1

3. Click **OK**.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

   Request timed out

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

   - Wrong physical connections
     - Make sure the LAN port light is on. If the light is off, follow the instructions in "LAN or Internet Port Lights Are Not On" on page 6-3".
     - Check that the corresponding link lights 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 computer 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 computer to a remote device. In the Windows Run window, 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 computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway. For more information, click the link to the online document "Preparing Your Network" in Appendix B.
- Check to see that the network address of your computer (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 computer, 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 computers. Many broadband ISPs restrict access by allowing only traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router with a specific MAC address in the Basic Settings screen. See "Basic Settings for Your Internet Connection" on page 1-6.

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 **192.168.1.1**. You can erase the current configuration and restore factory defaults in two ways:

- Erase the router configuration and return it to factory default settings. See "Erasing the Configuration" on page 4-2.
- Use the restore factory settings button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings when you do not know the administration password or IP address, use the restore settings button on the rear panel of the router.

1. Press and hold the restore settings button until the Test light blinks on (about 10 seconds).

2. Release the button, and wait for the router to reboot.

   If the wireless router fails to restart or the Power light continues to blink or turns solid amber, the unit could be defective. If the error persists, you might have a hardware problem and should contact Technical Support.

Problems with Date and Time

The E-Mail screen displays the current date and time of day. The wireless router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time can include the following:

- Date shown is January 1, 2000. Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least 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 E-Mail screen, select or clear the **Adjust for Daylight Savings Time** check box.

Appendix A
Technical Specifications and Default Configuration Settings

Technical Specifications

The following table provides technical specifications for the wireless router.

Table A-1. Technical Specifications

Data and Routing Protocols	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter	• North America: 120V, 60 Hz, input • United Kingdom, Australia: 240V, 50 Hz, input • Europe: 230V, 50 Hz, input • Japan: 100V, 50/60 Hz, input • All regions (output): 12V DC @ 1A output, 22W maximum
Physical Specifications	• Dimensions: 28 x 175 x 119 mm (1.1 x 6.89 x 4.68 in.) • Weight: 0.3 kg (0.66 lb)
Environmental Specifications	• Operating temperature: 0° to 40° C (32º to 104º F) • Operating humidity: 90% maximum relative humidity, noncondensing
Electromagnetic Emissions	Meets requirements of FCC Part 15 Class B.

Default Configuration Settings

The following table provides the factory default settings for the wireless router.

Table A-2. wireless router Default Configuration Settings

Feature		Default Setting
Smart Wizard		Enabled
Router login		
	Router login URLs	http://www.routerlogin.net http://www.routerlogin.com http://192.168.1.1
	User name (case-sensitive) printed on product label	admin
	Password (case-sensitive) printed on product label	password
Internet Connection		
	MAC address	Use default hardware address
Local Network		
	Router LAN IP address printed on product label	192.168.1.1
	Router subnet	255.255.255.0
	DHCP server	Enabled
	DHCP range	192.168.1.2 to 192.168.1.254
	Time zone	Pacific time
	Time zone adjusted for daylight saving time	Disabled
Wireless		
	Wireless communication	Enabled
	Wireless Access List (MAC Filtering)	All wireless stations allowed
	SSID name	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	802.11b/g RF Channel	6

Table A-2. wireless router Default Configuration Settings (continued)

Feature		Default Setting
	Transmission speed	Auto[a]
	Authentication type	Automatic
	Country/Region	United States in the U.S., otherwise varies by region
	RF channel	06
	Operating mode	Auto 108 Mbps
	Data rate	Best
	Output power	Full

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

Restoring the Default Settings

You can restore the factory default configuration settings to reset the router's user name to **admin,** the password to **password,** and the IP address to **192.168.1.1**. This procedure erases your current configuration, including your wireless security settings, and restores the factory defaults. When you log in after resetting, the Smart Wizard configuration assistant prompts you to configure these settings.

To restore the factory default configuration settings:

1. Use a sharp object such as a pen or a paper clip to press and hold the restore factory settings button, located on the rear panel of the router, for about 10 seconds.

2. Release the restore factory settings button, and wait for the router to reboot.

The factory default settings are restored so that you can access the router from your Web browser using the factory defaults.

Appendix B
Related Documents

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

Table B-1.

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*

Index