RangeMax Next Wireless Router WNR834B Reference Manual

NETGEAR

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

April 2006

© 2005 by NETGEAR, Inc. All rights reserved. April 2006.

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT 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.

Maximum Wireless Signal Rate Derived from IEEE Standard 802.11 Specifications

Actual data 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.

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

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

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

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Channel

You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available.

Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment.

European Union Statement of Compliance

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

Èesky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento RangeMax Next Wireless Router WNR834B je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr RangeMax Next Wireless Router WNR834B overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät RangeMax Next Wireless Router WNR834B in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme RangeMax Next Wireless Router WNR834B vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, NETGEAR, Inc., declares that this RangeMax Next Wireless Router WNR834B 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 RangeMax Next Wireless Router WNR834B 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 RangeMax Next Wireless Router WNR834B 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 RangeMax Next Wireless Router WNR834B 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 RangeMax Next Wireless Router WNR834B è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarç, ka RangeMax Next Wireless Router WNR834B atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis RangeMax Next Wireless Router WNR834B atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel RangeMax Next Wireless Router WNR834B 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 RangeMax Next Wireless Router WNR834B jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a RangeMax Next Wireless Router WNR834B megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oœwiadcza, ¿e RangeMax Next Wireless Router WNR834B jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este RangeMax Next Wireless Router WNR834B está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta RangeMax Next Wireless Router WNR834B v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že RangeMax Next Wireless Router WNR834B spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että RangeMax Next Wireless Router WNR834B tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the WNR834B product package.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das RangeMax Next Wireless Router WNR834B gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the RangeMax Next Wireless Router WNR834B has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example,

test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your RangeMax Next Wireless Router WNR834B.

World Wide Web

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

Product and Publication Details

Model Number:	WNR834B
Publication Date:	April 2006
Product Family:	Wireless Router
Product Name:	RangeMax Next Wireless Router WNR834B
Home or Business Product:	Home
Language:	English
Publication Part Number:	

Contents

RangeMax Next Wireless Router WNR834B Reference Manual

Chapter 1
About This Manual

Audience, Scope, Conventions, and Formats 1-1
How to Use This Manual 1-2
How to Print this Manual 1-2
Revision History 1-3

Chapter 2
Introduction

Package Contents 2-1
The Router's Front Panel 2-2
The Router's Rear Panel 2-3

Chapter 3
Connecting the Router to the Internet

Prepare to Install Your Wireless Router 3-1
First, Use the Smart Wizard to Configure the Wireless Router 3-2
Now, Set Up a Computer for Wireless Connectivity 3-2
Troubleshooting Tips 3-3
How to Manually Configure Your Internet Connection 3-6
Using the Smart Setup Wizard 3-9
NETGEAR Product Registration, Support, and Documentation 3-10

Chapter 4
Wireless Configuration

Observing Performance, Placement, and Range Guidelines 4-1
Implementing Appropriate Wireless Security 4-2
Understanding Wireless Settings 4-3
Information to Gather Before Changing Basic Wireless Settings 4-7
Default Factory Settings 4-8

How to Set Up and Test Basic Wireless Connectivity 4-9
How to Configure WEP 4-11
How to Configure WPA-PSK or WPA2-PSK Wireless Security 4-13
How to Restrict Wireless Access by MAC Address 4-15

Chapter 5
Content Filtering

Content Filtering Overview 5-1
Blocking Access to Internet Sites 5-2
Blocking Access to Internet Services 5-3
Configuring a User Defined Service 5-4
Blocking Services by IP Address Range 5-5
Scheduling When Blocking Will Be Enforced 5-5
Viewing Logs of Web Access or Attempted Web Access 5-6
Configuring E-Mail Alert and Web Access Log Notifications 5-7

Chapter 6
Maintenance

Viewing Wireless Router Status Information 6-1
Viewing a List of Attached Devices 6-5
Configuration File Management 6-5
Backing Up and Restoring the Configuration 6-6
Erasing the Configuration 6-6
Upgrading the Router Software 6-7
Changing the Administrator Password 6-9

Chapter 7
Advanced Configuration of the Router

Configuring Advanced Wireless Settings 7-1
Wireless Card Access List 7-3
Wireless Card Access Setup 7-4
Configuring Port Triggering and Port Forwarding 7-5
Configuring Port Forwarding to Local Servers 7-8
Adding a Custom Service 7-9
Editing or Deleting a Port Forwarding Entry 7-10
Local Web and FTP Server Example 7-10
Multiple Computers for Internet Gaming 7-10
Configuring the WAN Setup Options 7-11

Connecting Automatically, as Required 7-11
Disabling the SPI Firewall 7-12
Setting Up a Default DMZ Server 7-12
Responding to a Ping on the Internet WAN Port 7-12
Setting the MTU Size 7-13
Using the LAN IP Setup Options 7-13
Configuring LAN TCP/IP Setup Parameters 7-14
Using the Router as a DHCP server 7-15
Using Address Reservation 7-15
Using a Dynamic DNS Service 7-16
Configuring Static Routes 7-18
Enabling Remote Management Access 7-20
Using Universal Plug and Play (UPnP) 7-22

Chapter 8
Troubleshooting

Basic Functioning 8-1
Power Light Not On 8-1
Lights Never Turn Off 8-2
LAN or WAN Port Lights Not On 8-2
Troubleshooting the Web Configuration Interface 8-3
Troubleshooting the ISP Connection 8-4
Troubleshooting a TCP/IP Network Using a Ping Utility 8-5
Testing the LAN Path to Your Router 8-5
Testing the Path from Your Computer to a Remote Device 8-6
Restoring the Default Configuration and Password 8-7
Problems with Date and Time 8-8

Appendix A
Technical Specifications

Appendix B
Related Documents

Chapter 1
About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

Audience, Scope, Conventions, and Formats

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the NETGEAR website.

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

italics	Emphasis, books, CDs, URL names
bold	User input
`fixed`	Screen text, file and server names, extensions, commands, IP addresses

This guide uses the following formats to highlight special messages:

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

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

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

This manual is written for the WNR834B router according to these specifications:

Table 1-2. Manual Scope

Product Version	RangeMax Next Wireless Router WNR834B
Manual Publication Date	April 2006

Note: Product updates are available on the NETGEAR, Inc. web site at *http://kbserver.netgear.com/products/WNR834B.asp*

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A button that displays the table of contents and an index button. Double-click on 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 several options, according to your needs:

- **Printing a Page in the HTML View**.

  Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a 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 right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

> **Note:** Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

– Click the print icon in the upper left of the window.

> **Tip:** If your printer supports printing two pages on a single sheet of paper, you can select this feature to save paper and printer ink.

- **Printing the Full 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 the window.

> **Tip:** If your printer supports printing two pages on a single sheet of paper, you can select this feature to save paper and printer ink.

Revision History

NETGEAR, Inc. is constantly searching for ways to improve its products and documentation. The following table indicates any changes that may have been made since the WNR834B router was introduced.

Table 1-3. Publication Revision History

Version	Date	Description
v1.0	November 2005	Original publication
v1.1	January 2006	A number of technical corrections were incorporated into chapters 2, 3, 4, 6, and Appendix A.

Chapter 2
Introduction

Congratulations on your purchase of the NETGEAR® RangeMax Next Wireless Router WNR834B. The WNR834B router provides connection for multiple computers to the Internet through an external broadband access device (such as a cable modem or DSL modem) that is normally intended for use by a single computer.

Package Contents

The product package should contain the following items:

- RangeMax Next Wireless Router WNR834B
- AC power adapter
- Vertical stand
- Category 5 (CAT5) Ethernet cable
- *Resource CD*, including:
  - The Setup manual
  - Application Notes and other helpful information
- *Wireless Home Router Setup Guide*
- Warranty and Support Information Card
- Detachable antenna

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

The Router's Front Panel

The front panel of the WNR834B router contains the status lights described below.

You can use the status lights to verify connections. Viewed from left to right, the table below describes the lights on the front panel of the router.

Table 2-1. Status Light Descriptions

Item	Function	Activity	Description
1	Power	On	Power is supplied to the router.
		Off	Power is not supplied to the router.
2	Wireless	On	The wireless interface is enabled.
		Off	The wireless interface is turned off.
		Blinking	Data is being communicated over the wireless network.
3	Internet Port	Amber Off	No Ethernet cable is connected to the modem.
		Amber On	Ethernet cable connection to modem is good.
		Amber blinking	Packets are being transmitted and received from a modem or other network device, but no IP address has been received.
		Green off	No IP address received.
		Green on	IP address received.
		Blink	IP address received and data is being transmitted and received.
4	LAN Ports	Green	The LAN port has detected a 100 Mbps link with an attached device.
		Amber	The LAN port has detected a 10 Mbps link with an attached device

The Router's Rear Panel

The rear panel of the WNR834B router contains the items listed below.

Viewed from top to bottom, the rear panel contains the following features:

1. Factory Default Reset push button for "Restoring the Default Configuration and Password" on page 8-7.
2. Four Local (LAN) 10/100 Mbps Ethernet ports for connecting the router to the local computers.
3. Internet (WAN) Ethernet port for connecting the router to a cable or DSL modem.
4. AC power adapter outlet.

Chapter 3
Connecting the Router to the Internet

This chapter describes how to set up the router on your local area network (LAN) and connect to the Internet. You will find out how to configure your RangeMax Next Wireless Router WNR834B for Internet access using the Setup Wizard, or how to manually configure your Internet connection.

Follow these instructions to set up your router.

Prepare to Install Your Wireless Router

- Observe the wireless placement and range guidelines in *"Observing Performance, Placement, and Range Guidelines" on page 4-1*.
- *For Cable Modem Service*: When you perform the wireless router setup steps, be sure to use the computer you first registered with your cable ISP.
- *For DSL Service*: You may need information such as the DSL login name/e-mail address and password in order to complete the wireless router setup.

Before proceeding with the wireless router installation, familiarize yourself with the contents of the *Resource CD*, especially this manual and the animated tutorials for configuring networking on PCs.

First, Use the Smart Wizard to Configure the Wireless Router

Insert the *Resource CD* in the CD drive of your PC. The following screen appears. Click **SETUP** and follow the prompts.

Now, Set Up a Computer for Wireless Connectivity

You are now connected to the Internet and the wireless feature of the wireless router is enabled! Next, configure your wireless computer.

1. Configure the computer's Wireless Adapter settings.

Wireless Adapter in a Notebook Computer

Figure 3-1

NETGEAR, Inc. wireless adapters display a list of available wireless networks and, when wireless security is disabled, you simply choose yours from the list and connect.

For a non-NETGEAR wireless adapter, configure it to match your settings exactly. If you changed the default Network Name (SSID), be sure to use the correct Network Name (SSID) you set in the wireless router.

WIRELESS FEATURE	DEFAULT SETTING
Network Name (SSID)	**NETGEAR**
WEP Security	**Disabled**

Warning: The Network Name (SSID) is case sensitive. Typing nETgear will not work.

2. Verify wireless connectivity.

Verify wireless connectivity. Connect to the Internet or log in to the wireless router from a computer with a wireless adapter. For wireless connectivity problems, see "Troubleshooting Tips" on page 3-3.

You are now wirelessly connected to the Internet! Implement wireless security according to the instructions in "Implementing Appropriate Wireless Security" on page 4-2.

Troubleshooting Tips

Here are some tips for correcting simple problems you may have:

Be sure to restart your network in this sequence:

1) Turn off the modem, wireless router, and computer; 2) Turn on the modem, wait two minutes; 3) Turn on the wireless router and wait 1 minute; 4) Turn on the computer.

Make sure the Ethernet cables are securely plugged in.

- The Internet status light on the wireless router will be lit if the Ethernet cable to the wireless router from 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 with a securely plugged in Ethernet cable, the corresponding wireless router LAN port status light will be lit. The label on the bottom of the wireless router identifies the number of each LAN port.

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

The Wireless Network Name (SSID) and WEP or WPA security settings of the router and wireless computer must match exactly.

Make sure the network settings of the computer are correct.

- LAN and wirelessly connected computers *must* be configured to obtain an IP address automatically via DHCP. Please see "Preparing a Computer for Network Access" in Appendix B or the animated tutorials on the CD for help with this.
- Some cable modem ISPs require you to use the MAC address of the computer registered on the account. If so, in the Router MAC Address section of the Basic Settings menu, select **Use this Computer's MAC Address**. The router will then capture and use the MAC address of the computer that you are now using. You must be using the computer that is registered with the ISP. Click **Apply** to save your settings. Restart the network in the correct sequence.

How to Log On to the Wireless Router After Configuration Settings Have Been Applied

1. Connect to the wireless router by typing *http://www.routerlogin.net* in the address field of your browser, then click **Enter**.

Figure 3-2

2. For security reasons, the router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 6-9.

   Note: The router user name and password are not the same as any user name or password you may use to log in to your Internet connection.

Figure 3-3

Once you have entered your user name and password, your Web browser should find the WNR834B router and display the home page as shown in Figure 3-4 below.

	Note: If the **Check for New Version Upon Log-in** checkbox is checked, the home page will be the Router Upgrade page. Otherwise, it will be the Basic Settings page.

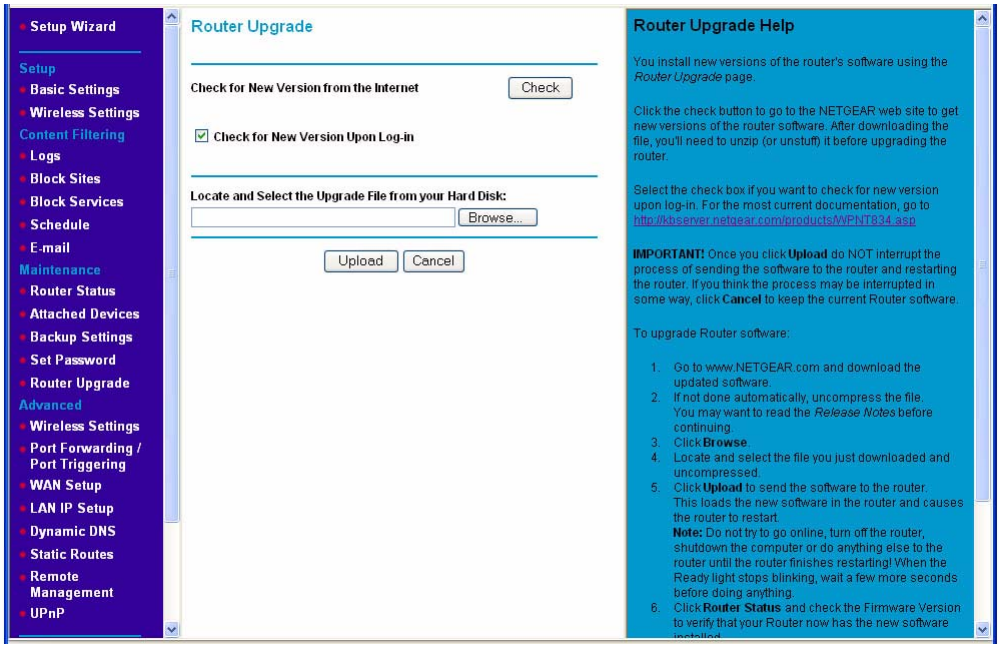


Figure 3-4

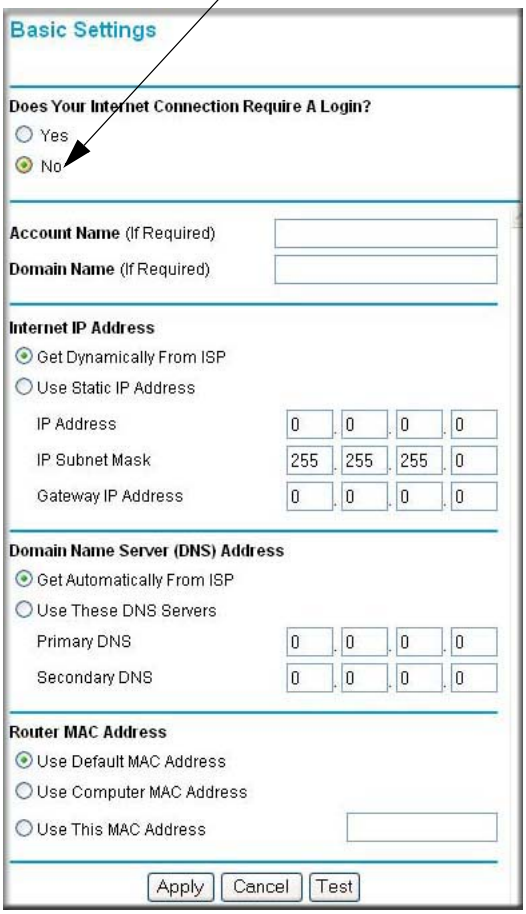
When the wireless router is connected to the Internet, click the **Knowledge Base** or the **Documentation** link under the Web Support menu to view support information or the documentation for the wireless router.

If you do not click **Logout**, the wireless router will wait 5 minutes after there is no activity before it automatically logs you out.

How to Manually Configure Your Internet Connection

You can manually configure your router using the Basic Settings menu, shown below, or you can allow the Setup Wizard to determine your configuration as described in the previous section.

ISP *Does Not* Require Login



ISP *Does* Require Login

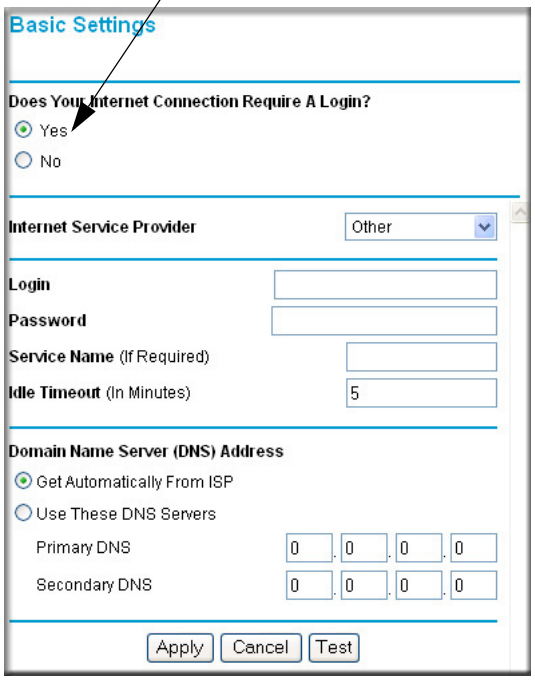


Figure 3-5

You can manually configure the router using the Basic Settings menu shown in Figure 3-5 using these steps:

1. Connect to the wireless router by typing *http://www.routerlogin.net* in the address field of your browser, then click **Enter**.

2. For security reasons, the wireless router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters.
3. Click **Basic Settings** on the Setup menu.
4. If your Internet connection does not require a login, click **No** at the top of the Basic Settings menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click **Yes**, and skip to step 5.

   a. Enter your Account Name (may also be called Host Name) and Domain Name.
   These parameters may be necessary to access your ISP's services such as mail or news servers.

   b. Internet IP Address:
   If your ISP has assigned you a permanent, fixed (static) IP address for your computer, select **Use Static IP Address**. Enter the IP address that your ISP assigned. Also enter the net mask and the Gateway IP address. The Gateway is the ISP's router to which your router will connect.

   c. Domain Name Server (DNS) Address:
   If you know that your ISP does not automatically transmit DNS addresses to the router during login, select **Use These DNS Servers** and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

	Note: If you enter an address here, restart the computers on your network so that these settings take effect.

   d. Router's MAC Address:
   This section determines the Ethernet MAC address that will the router will use on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by "cloning" its MAC address.

   To change the MAC address, select **Use Computer MAC Address**. The router will then 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. Or, select **Use this MAC address** and type it in here.

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

5. If your Internet connection does require a login, fill in the settings according to the instructions below. Select **Yes** if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.

	Note: After you finish setting up your router, you will no longer need to launch the ISP's login program on your computer in order to access the Internet. When you start an Internet application, your router will automatically log you in.

a. Select your Internet service provider from the drop-down list.

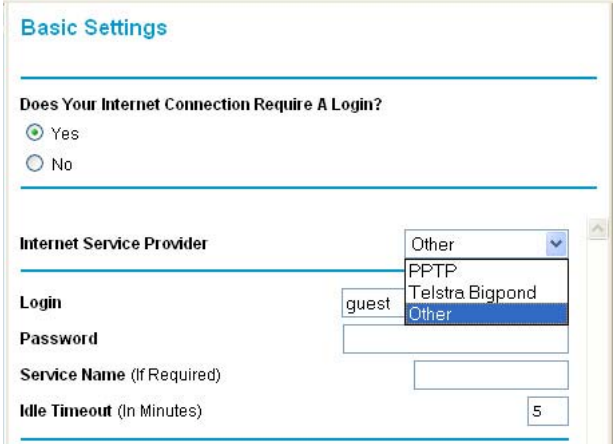


Figure 3-6

	Note: Not all ISPs are listed here. The ones on this list have special requirements.

b. The screen will change according to the ISP settings requirements of the ISP you select.

c. Fill in the parameters for your Internet service provider.

d. Click **Apply** to save your settings. Click the **Test** button to verify you have Internet access.

Using the Smart Setup Wizard

You can use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection. The Smart Setup Wizard is not the same as the Smart Wizard configuration assistant (as illustrated in Figure 3-1) that only appears when the router is in its factory default state. After you configure the wireless router, the Smart Wizard configuration assistant will not appear again.

To use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection settings, follow this procedure:

1. Connect to the wireless router by typing *http://www.routerlogin.net* in the address field of your browser, then click **Enter**.
2. For security reasons, the router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 6-9.

	Note: The router user name and password are not the same as any user name or password you may use to log in to your Internet connection.

   Once you have entered your user name and password, your Web browser should find the WNR834B router and display the home page as shown in Figure 3-4 on page 3-5.

3. Click **Setup Wizard** on the upper left of the main menu.
4. Click **Next** to proceed. Input your ISP settings, as needed.
5. At the end of the Setup Wizard, click the **Test** button to verify your Internet connection. If you have trouble connecting to the Internet, use the "Troubleshooting Tips" on page 3-3 to correct basic problems, or see Chapter 8, "Troubleshooting".

NETGEAR Product Registration, Support, and Documentation

Register your product at *http://www.netgear.com/register*. Registration is required before you can use our telephone support service.

Product updates and Web support are always available by going to: *http://kbserver.netgear.com/products/WNR834B.asp*.

Documentation is available on the CD and at *http://kbserver.netgear.com/documentation/WNR834B.asp*

When the wireless router is connected to the Internet, click the **Knowledge Base** or the **Documentation** link under the Web Support menu to view support information or the documentation for the wireless router.

Chapter 4
Wireless Configuration

This chapter describes how to configure the wireless features of your WNR834B router. In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your firewall in order to maximize the network speed. For further information on wireless networking, see "Wireless Communications" in Appendix B.

Observing Performance, Placement, and Range Guidelines

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

	Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range and performance specifications, please see Appendix A, "Technical Specifications".

For best results, place your firewall:

- 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, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP, WPA-PSK and WPA2-PSK encryption can consume more battery power on a notebook computer.

Implementing Appropriate Wireless Security

	Note: Indoors, computers can connect over 802.11b/g wireless networks at ranges of up to 300 feet. Such distances can allow for others outside of your immediate area to access your network.

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 WNR834B router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

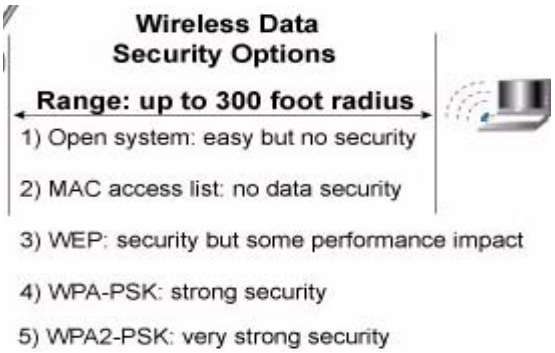


Figure 4-1

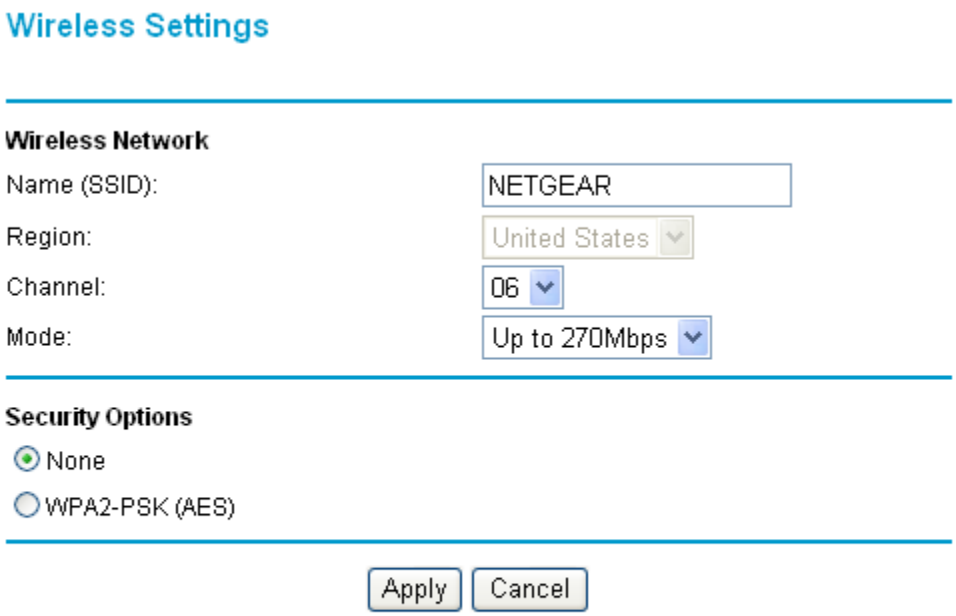
There are several ways you can enhance the security of your wireless network.

- **Restrict Access Based on MAC address.** You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WNR834B. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies 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.
- **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.

- **WPA-PSK** and **WPA2-PSK.** Wi-Fi Protected Access, Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provide strong data security. WPA-PSK and WPA2-PSK block eavesdropping. Because these are new standards, wireless device driver and software availability may be limited.
- **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 other users of your network all use wired connections.

Understanding Wireless Settings

To configure the Wireless settings of your firewall, click the **Wireless** link in the main menu of the browser interface. The Wireless Settings menu appears, as shown below.



- **Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. 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 particular wireless network will need to use this SSID for that network. The WNR834B default SSID is: **NETGEAR**.
- **Region.** This field identifies the region where the WNR834B can be used. It may not be legal to operate the wireless features of the wireless router in a region other than one of those identified in this field.

	Note: The region selection feature may not be available in all countries.

- **Channel.** This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point. For more information on the wireless channel frequencies, see "Wireless Communications" in Appendix B.
- **Mode.** This field determines which data communications protocol is used. You can select "g only", "g and b", "Up To 130 Mbps", and "Up To 270 MBps". The "g only" option dedicates the WNR834B to communicating with the higher bandwidth 802.11g wireless devices exclusively. The "g and b" mode provides backward compatibility with the slower 802.11b wireless devices while still enabling 802.11g communications. The "Up to 130 Mbps" mode provides two transmission streams with different data on the same channel at the same time. The "Up to 270 Mbps" uses channel expansion to achieve the 270 Mbps data rate. The WNR834B router will use the channel you selected as the primary channel and expand to the secondary channel (primary channel +4 or -4) to achieve a 40MHz frame-by-frame bandwidth. The WNR834B router will detect channel usage and will disable frame-by-frame expansion if the expansion would result in interference with the data transmission of other access points or clients.

	Note: The maximum wireless signal rate is derived from the IEEE Standard 802.11 Specifications. Actual data 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.

- **Security Options.** These options are the wireless security features you can enable. The table below identifies the various basic wireless security options. A full explanation of these standards is available in "Wireless Communications" in Appendix B.

Table 4-1. Basic Wireless Security Options

Field	Description
None	No wireless security.
WEP	WEP offers the following options: • Open System With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the WNR834B *does* perform 64- or 128-bit data encryption but *does not* perform any authentication. • Shared Key Shared Key authentication encrypts the SSID and data. Choose the Encryption Strength (64- or 128-bit data encryption). Manually enter the key values or enter a word or group of printable characters in the Passphrase box. Manually entered keys *are* case sensitive but passphrase characters *are not* case sensitive. **Note**: Not all wireless adapter configuration utilities support passphrase key generation. • Auto The wireless router automatically detects whether Open System or Shared Key is used.
WPA-PSK **WPA2-PSK**	WPA-Pre-shared Key *does* perform authentication. WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption and WPA2-PSK uses AES (Advanced Encryption Standard) data encryption. Both dynamically change the encryption keys making them nearly impossible to circumvent. Enter a word or group of printable characters in the Password Phrase box. These characters *are* case sensitive. **Note**: Not all wireless adapter configuration utilities support WPA-PSK and WPA2-PSK. Furthermore, client software is required on the client. Windows XP Service Pack 2 and Windows XP Service Pack 1 with WPA patch do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.

To configure the advanced wireless settings of your firewall, click the **Wireless Setup** link in the Advanced section of the main menu of the browser interface. The Advanced Wireless Settings menu appears, as shown below.

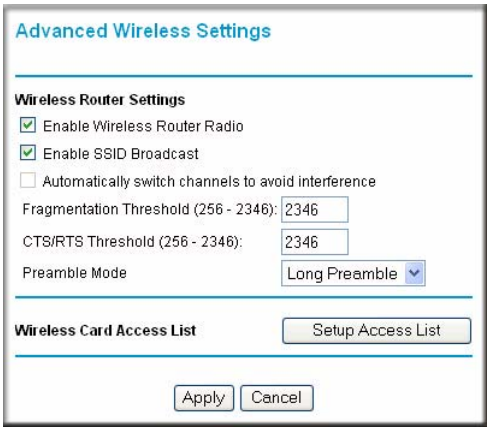


Figure 4-3

- **Enable Wireless Router Radio.** If you disable the wireless router radio, wireless devices cannot connect to the WNR834B.
- **Enable SSID Broadcast.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network ‘discovery’ feature of some products such as Windows XP.
- **Automatically switch channels to avoid interference.** If enabled, the WNR834B router will periodically survey the wireless environment to ensure that it is using the clearest channel. If a clearer channel is available, it may automatically switch channels.

	Note: After the router switches channels, there may be a slight delay while your wireless computers reconnect to the router. If you want to avoid this possibility, leave this checkbox unselected.

- **Wireless Card Access List.** When the Trusted PCs Only radio button is selected, the WNR834B checks the MAC address of the wireless station and only allows connections to computers identified on the trusted computers list.

	Note: The **Fragmentation Threshold**, **CTS/RTS Threshold**, and **Preamble Mode** options are reserved for wireless testing and advanced configuration only. Do not change these settings.

Information to Gather Before Changing Basic Wireless Settings

Before customizing your wireless settings, print this form and record the following information. If you are working with an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Otherwise, you must choose the settings for your wireless network. Either way, record the settings for your wireless network in the spaces below.

- **Wireless Network Name (SSID)*:*** _____ The SSID identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID *is* case sensitive. The SSID in the wireless adapter card 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**.

	Note: If you select **Shared Key**, the other devices in the network will not connect unless they are also set to Shared Key and are configured with the correct key.

  – **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 or a-f). For 128-bit WEP, enter 26 hex digits.

    Key 1: _____

    Key 2: _____

    Key 3: _____

    Key 4: _____

- **If WPA-PSK or WPA2-PSK Authentication is Used:**
  - **Passphrase**: _____ These characters *are* case sensitive. Enter a word or group of printable characters. When you use WPA-PSK, the other devices in the network will not connect unless they are set to WPA-PSK as well and are configured with the correct Passphrase. Similarly, when you use WPA2-PSK, the other devices in the network will not connect unless they are also set to WPA2-PSK and are configured with the correct Passphrase.

Use the procedures described in the following sections to configure the WNR834B. Store this information in a safe place.

Default Factory Settings

When you first receive your WNR834B, the default factory settings are in effect, as shown below. You can restore these defaults with the Factory Default Restore button on the rear panel. After you install the WNR834B router, use the procedures below to customize any of the settings to better meet your networking needs.

FEATURE	DEFAULT FACTORY SETTINGS
Wireless Router Radio	**Enabled**
Wireless Access List (MAC Filtering)	**All wireless stations allowed**
SSID broadcast	**Enabled**
SSID	**NETGEAR**
802.11b/g RF Channel	**Auto**
Security	**None**
DHCP Server	**Enabled**
DHCP range	**192.168.1.2 to 192.168.1.254**

How to Set Up and Test Basic Wireless Connectivity

	Note: If you use a wireless computer to configure WPA settings, you will be disconnected when you click **Apply**. Reconfigure your wireless adapter to match the new settings or access the wireless router from a wired computer to make any further changes.

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in to the WNR834B firewall at its default LAN address of *http://www.routerlogin.net* (or *http://192.168.1.1*) with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the main menu of the WNR834B firewall.

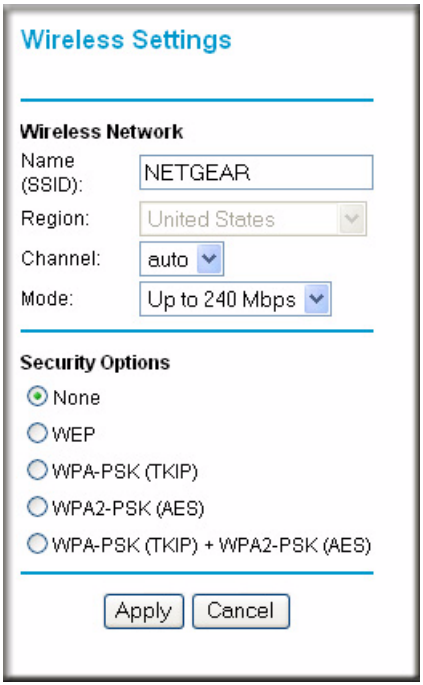


Figure 4-4

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

	Note: The SSID is case sensitive; NETGEAR is not the same as nETgear. Also, the SSID of any wireless access adapters must match the SSID you configure in the RangeMax Next Wireless Router WNR834B. If they do not match, you will not get a wireless connection to the WNR834B.

4. Set the Region. Select the region in which the wireless interface will operate.
5. Set the Channel. The default channel is Auto.

   This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your firewall. For more information on the wireless channel frequencies, see "Wireless Communications" in Appendix B.
6. For initial configuration and testing, leave the Wireless Card Access List set to "Everyone" and the Encryption Strength set to "Disabled."
7. Click **Apply** to save your changes.

	Note: If you are configuring the firewall from a wireless computer and you change the firewall's SSID, channel, or security settings, you will lose your wireless connection when you click **Apply**. You must then change the wireless settings of your computer to match the firewall's new settings.

8. Configure and test your computers for wireless connectivity.

   Program the wireless adapter of your computers to have the same SSID and channel that you configured in the router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the firewall.

	Warning: The Network Name (SSID) is case sensitive. If NETGEAR is the Network Name (SSID) in your wireless router, you must enter NETGEAR in your computer's wireless settings. Typing nETgear will not work.

Once your computers have basic wireless connectivity to the firewall, you can configure the advanced wireless security functions of the firewall.

How to Configure WEP

To configure WEP data encryption, follow these steps:

	Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click **Apply**. You must then either configure your wireless adapter to match the wireless router WEP settings or access the wireless router from a wired computer to make any further changes.

1. Log in to the WNR834B firewall at its default LAN address of *http://www.routerlogin.net* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the main menu of the WNR834B firewall.
3. From the Security Options menu, select **WEP**. The WEP options display.

4. Select the Authentication Type and Encryptions strength from the drop-down lists.

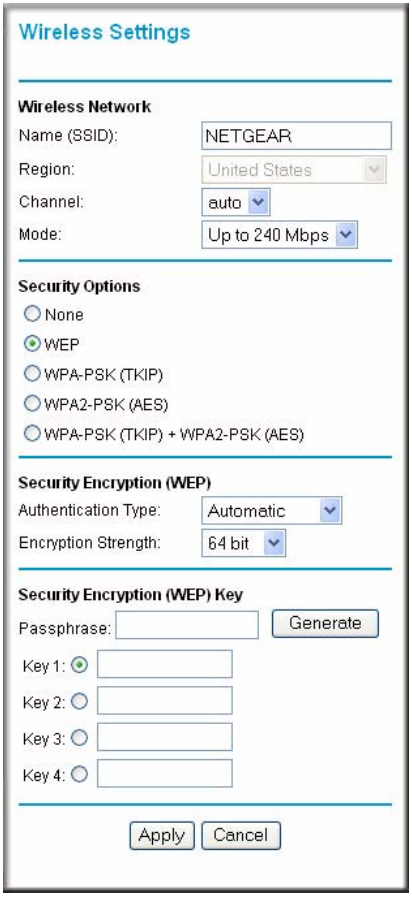


Figure 4-5

5. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network.

- Automatic—Enter a word or group of printable characters in the Passphrase box and click the **Generate** button. The passphrase is case sensitive; NETGEAR is not the same as nETgear. The four key boxes is automatically populated with key values.
- Manual—Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F). These entries are not case sensitive; AA is the same as aa.
  Select which of the four keys to activate.

See "Wireless Communications" in Appendix B for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

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

How to Configure WPA-PSK or WPA2-PSK Wireless Security

	Note: Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP with Service Pack 2 does include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless computers or PDAs (Personal Digital Assistants) for WPA-PSK security, consult the documentation for the product you are using.

To configure WPA-PSK or WPA2-PSK, follow these steps:

1. Click **Wireless Settings** in the Setup section of the main menu and select one of the WPA-PSK or WPA2-PSK options for the Security Type. The third option (**WPA-PSK [TKIP] + WP2-PSK [AES]**) is the most flexible, since it allows clients using either WPA-PSK or WPA2-PSK.

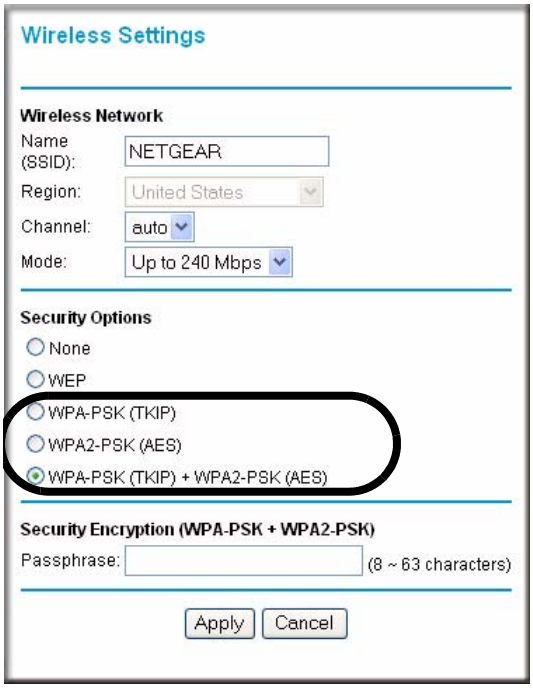


Figure 4-6

2. Enter a word or group of 8-63 printable characters in the Passphrase box.
3. Click **Apply** to save your settings.

How to Restrict Wireless Access by MAC Address

To restrict access based on MAC addresses, follow these steps:

1. Log in to the WNR834B firewall at its default LAN address of *http://www.routerlogin.net* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

> **Note:** When configuring the firewall from a wireless computer whose MAC address is not in the Trusted PC list, if you select **Turn Access Control On**, you will lose your wireless connection when you click **Apply**. You must then access the wireless router from a wired computer or from a wireless computer which is on the access control list to make any further changes.

2. Click **Wireless Settings** in the **Advanced** section of the main menu of the WNR834B firewall.
3. From the Wireless Settings menu, click **Setup Access List** to display the Wireless Access menu shown below.

Figure 4-7

4. Click the **Turn Access Control On** check box.

5. Click **Add** to add a wireless device to the wireless access control list. The Wireless Card Access Setup dialog displays.

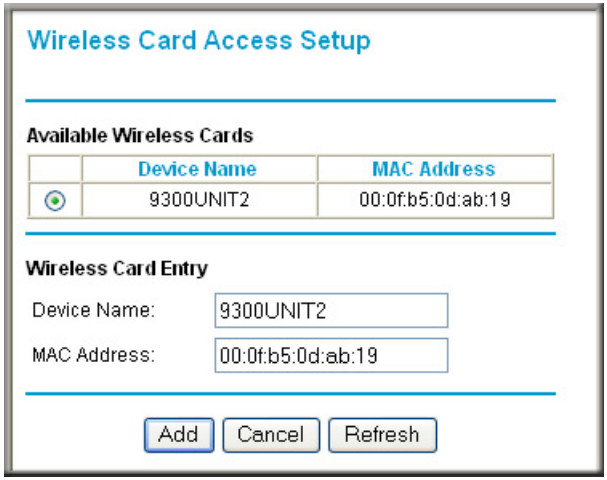


Figure 4-8

6. In the Available Wireless Cards list, either select from the list of available wireless cards the WNR834B has found in your area, or enter the MAC address and device name for a device you plan to use. You can usually find the MAC address printed on the wireless adapter.

	Note: You can copy and paste the MAC addresses from the firewall's Attached Devices menu into the MAC Address box of this menu. To do this, configure each wireless computer to obtain a wireless link to the firewall. The computer should then appear in the Attached Devices menu.

7. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.
8. Repeat step 5 to step 7 for each additional device you wish to add to the list.
9. Be sure to click **Apply** to save your Wireless Card Access List settings.

Now, only devices on this list are allowed to wirelessly connect to the WNR834B.

Chapter 5
Content Filtering

This chapter describes how to use the content filtering features of the RangeMax Next Wireless Router WNR834B to protect your network. These features can be found by clicking on the **Content Filtering** heading in the main menu of the browser interface.

Content Filtering Overview

The RangeMax Next Wireless Router WNR834B provides you with Web content filtering options, plus browser 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.

To configure these features of your router, click on the subheadings under the **Content Filtering** heading in the main menu of the browser interface. The subheadings are described below:

Blocking Access to Internet Sites

The WNR834B router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is shown in the figure below:

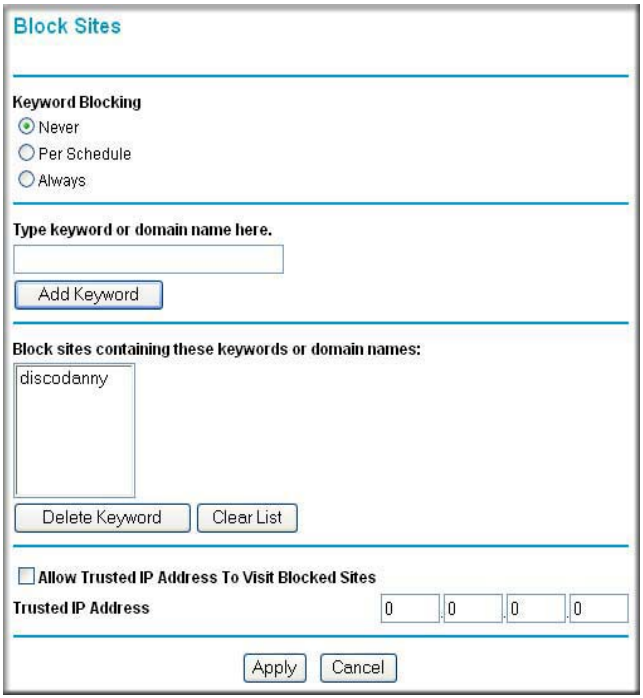


Figure 5-1

To enable keyword blocking, select either **Per Schedule** or **Always**, then click **Apply**. If you want to block by schedule, be sure to specify a time period in the Schedule menu. For scheduling, see "Scheduling When Blocking Will Be Enforced" on page 5-5.

To add a keyword or domain, type it in the Keyword box, click **Add Keyword**, then click **Apply**.

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

Keyword application examples:

- If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the keyword ".com" is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.

- If you wish to block all Internet browsing access during a scheduled period, enter the keyword "." and set the schedule in the Schedule menu.

To specify a Trusted User, enter that computer's IP address in the Trusted User box and click **Apply**.

You may specify one Trusted User, which is a computer that is exempt from blocking and logging. Since the Trusted User is identified by IP address, you should configure that computer with a fixed IP address.

Blocking Access to Internet Services

The WNR834B router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. The Block Services menu is shown below:

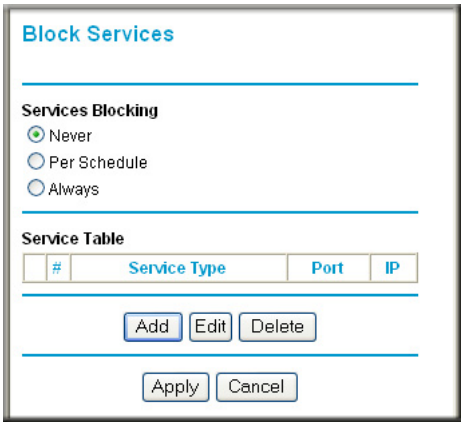


Figure 5-2

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.

To enable service blocking, select either **Per Schedule** or **Always**, then click **Apply**. If you want to block by schedule, be sure to specify a time period in the Schedule menu. For scheduling, see "Scheduling When Blocking Will Be Enforced" on page 5-5.

To specify a service for blocking, click **Add**. The Block Services Setup menu appears, as shown below:

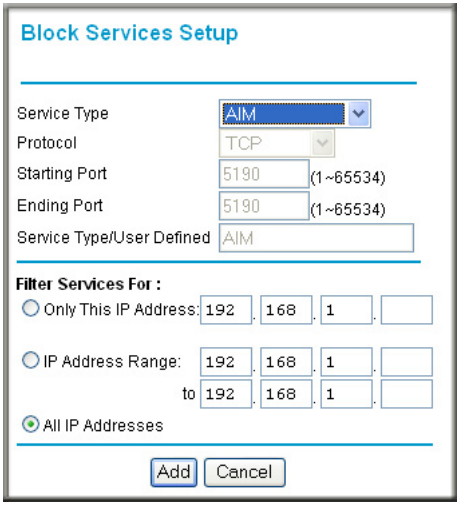


Figure 5-3

From the **Service Type** list, select the application or service to be allowed or blocked. The list already displays several common services, but you are not limited to these choices. To add any additional services or applications that do not already appear, select **User Defined**.

Configuring a User Defined Service

To define a service, first you must determine which port number or range of numbers is used by the application. 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.

Enter the Starting Port and Ending Port numbers. If the application uses a single port number, enter that number in both boxes.

If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select **Both**.

Blocking Services by IP Address Range

Under “Filter Services For”, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Scheduling When Blocking Will Be Enforced

The WNR834B router allows you to specify when blocking is enforced. The Schedule menu is shown below:

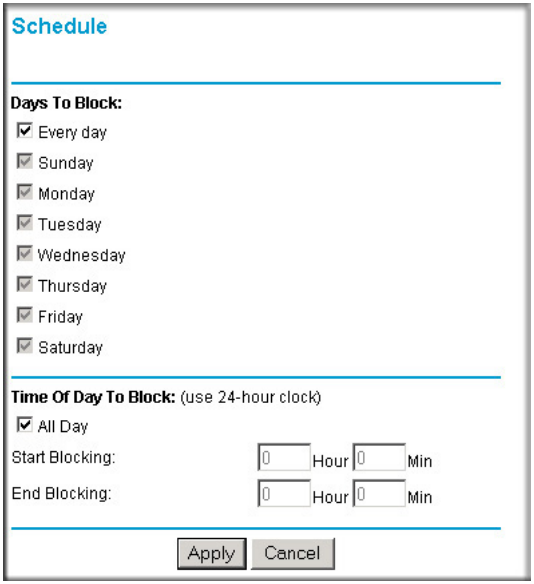


Figure 5-4

Use this schedule for blocking content.

- Days to Block. Select days to block by checking the appropriate boxes. Select **Every day** to check the boxes for all days. Click **Apply**.
- Time of Day to Block. Select a start and end time in 24-hour format. Select **All day** for 24-hour blocking. Click **Apply**.

Be sure to select your Time Zone in the E-Mail menu.

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of the Web sites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries only appear when keyword blocking is enabled, and no log entries are made for the Trusted User. An example is shown below:

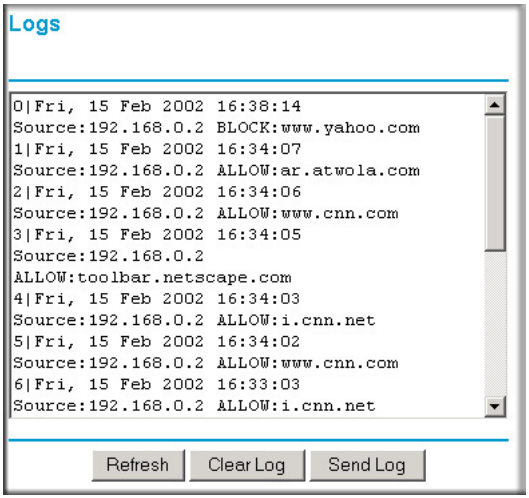


Figure 5-5

Log entries are described in the following table.

Table 5-1. Log entry descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Source IP	The IP address of the initiating device for this log entry.
Target address	The name or IP address of the Web site or newsgroup visited or attempted to access.
Action	This field displays whether the access was blocked or allowed.

Log action buttons are described in the following table.

Table 5-2. Log action buttons

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to E-mail the log immediately.

Configuring E-Mail Alert and Web Access Log Notifications

In order to receive logs and alerts by E-mail, you must provide your E-mail information in the E-Mail menu, shown below:

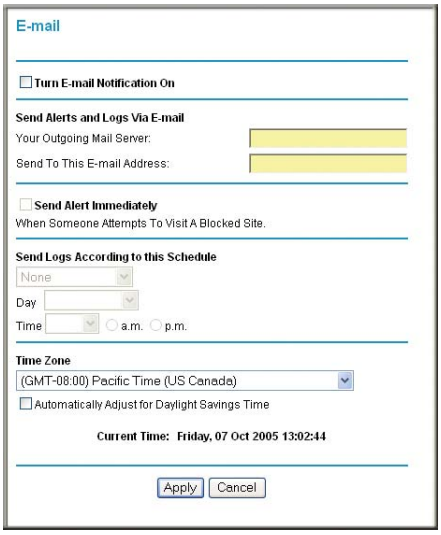


Figure 5-6

- Turn e-mail notification on.
  Check this box if you wish to receive e-mail logs and alerts from the router.
- Your outgoing mail server .
  Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.

- Send to this e-mail address .
  Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.

You can specify that logs are automatically sent to the specified e-mail address with these options:

- Send alert immediately.
  Check this box if you would like immediate notification of 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, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents.

The WNR834B router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

- Time Zone.
  Select your local time zone. This setting is used for the blocking schedule and for time-stamping log entries.
- Adjust for Daylight Savings Time.
  Check this box if your time zone is currently under daylight savings time.

Chapter 6
Maintenance

This chapter describes how to use the maintenance features of your RangeMax Next Wireless Router WNR834B. These features can be found by clicking on the **Maintenance** heading in the main menu of the browser interface.

Viewing Wireless Router Status Information

The Router Status menu provides status and usage information. From the main menu of the browser interface, click **Maintenance**, then select **Router Status** to view the Router Status screen, shown below.

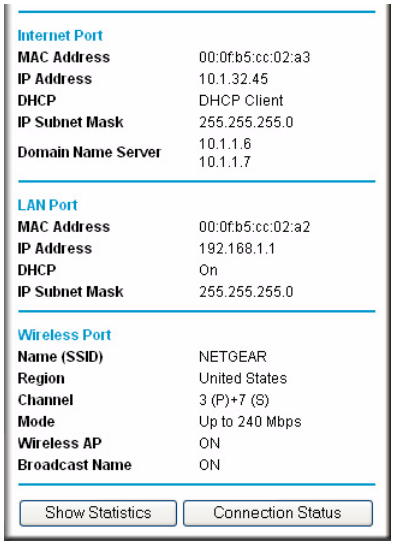


Figure 6-1

This screen shows the following parameters:

Table 6-1. Wireless Router Status Fields

Field	Description
Account Name	This field displays the Host Name assigned to the router.
Firmware Version	This is the version of the current software the router is using. This will change if you upgrade your router.
Internet Port	These parameters apply to the Internet (WAN) port of the router.
MAC Address	This field displays the Media Access Control address, the physical address, being used by the Internet (WAN) port of the router.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, or is 0.0.0.0, the router cannot connect to the Internet.
DHCP	If set to None, the router is configured to use a fixed IP address on the WAN. If set to DHCP Client, the router is configured to obtain an IP address dynamically from the ISP.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router. For an explanation of subnet masks and subnet addressing, see "Internet Networking and TCP/IP Addressing" in Appendix B.
Domain Name Server	This field displays the Domain Name Server addresses being used by the router. A Domain Name Server translates human-language URLs, such as http://www.netgear.com, into IP addresses.
LAN Port	These parameters apply to the Local (LAN) port of the router.
MAC Address	This field displays the Media Access Control address, the physical address, being used by the LAN port of the router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.1.1
DHCP	Identifies if the router's built-in DHCP server is active for the LAN attached devices.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0

Table 6-1. Wireless Router Status Fields (continued)

Field	Description
Wireless Port	These parameters apply to the Wireless port of the router.
Name (SSID)	This field displays the wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR.
Region	This field displays the geographic region where the router being used. It may be illegal to use the wireless features of the router in some parts of the world.
Channel	Identifies the channel of the wireless port being used. See "Wireless Communications" in Appendix B for the frequencies used on each channel. In "Up to 270 Mbps" mode, there are two channels: a primary channel (P) and a secondary channel (S).
Mode	Indicates the router communication mode: 802.11g and 802.11b, 802.11g only, Up To 130 Mbps, or Up To 270 Mbps.
Wireless AP	Indicates if the Router Radio feature of the Router is enabled. If not enabled, the Wireless LED on the front panel will be off.
Broadcast Name	Indicates if the router is broadcasting its SSID

Click on the **Connection Status** button to display the connection status, as shown below.

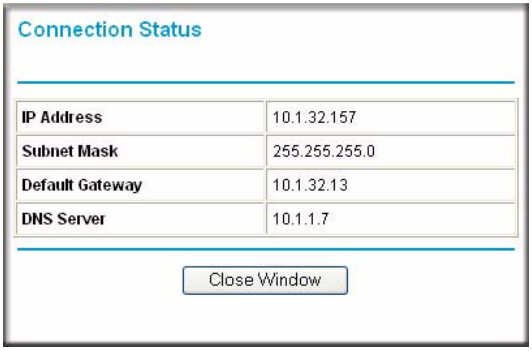


Figure 6-2

This screen shows the following statistics:.

Table 6-2: Connection Status Items

Item	Description
IP Address	The WAN (Internet) IP Address assigned to the router.
Subnet Mask	The WAN (Internet) Subnet Mask assigned to the router.
Default Gateway	The WAN (Internet) default gateway the router communicates with.
DNS Server	The IP address of the DNS server which provides network name to IP address translation.

Click the **Show Statistics** button to display router usage statistics, as shown below.

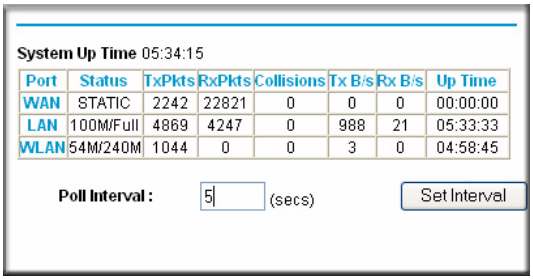


Figure 6-3

This screen shows the following statistics:

Table 6-3: Router Statistics Items

Item	Description
System Up Time	The amount of time since the router was last restarted.
Port	The statistics for the WAN (Internet) and LAN (local) ports. For each port, the screen displays:
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 transmission (outbound) bandwidth used on the WAN and LAN ports.
Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.

Table 6-3: Router Statistics Items (continued)

Item	Description
Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window.
Set Interval	Enter a time and click the **Set Interval** button to set the polling frequency.

Viewing a List of Attached Devices

The Attached Devices menu contains a table of all IP devices that the router has discovered on the local network. From the main menu of the browser interface, under the Maintenance heading, select **Attached Devices** to view the table, shown below.

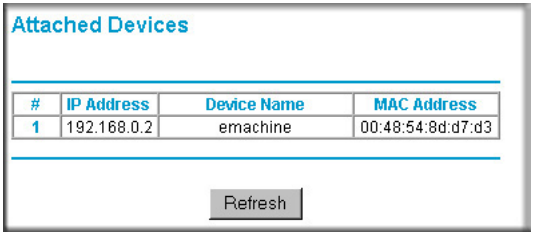


Figure 6-4

For each device, the table shows the IP address, NetBIOS Host Name or Device Name (if available), and Ethernet MAC address. To force the router to look for attached devices, click the **Refresh** button.

Note: If the router is rebooted, the table data is lost until the router rediscovers the devices.

Configuration File Management

The configuration settings of the WNR834B router are stored within the router in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

From the main menu of the browser interface, under the Maintenance heading, select the **Backup Settings** heading to bring up the menu shown below.

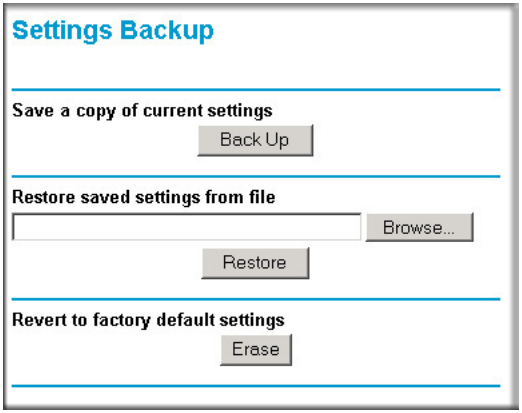


Figure 6-5

Three options are available, and are described in the following sections.

Backing Up and Restoring the Configuration

The Restore and Backup options in the Settings Backup menu allow you to save and retrieve a file containing your router's configuration settings.

To save your settings, click the **Back Up** button. Your browser will extract the configuration file from the router and will prompt you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as pacbell.cfg.

To restore your settings from a saved configuration file, enter the full path to the file on your computer or click the **Browse** button to browse to the file. When you have located it, click the **Restore** button to send the file to the router. The router will then reboot automatically.

⚠	**Warning:** Do not interrupt the reboot process.

Erasing the Configuration

It is sometimes desirable to restore the router to the original default settings. This can be done using the Erase function, which restores all factory settings. After an erase, the router's username is **admin**, the password is **password**, the LAN IP address is192.168.1.1, and the router's DHCP server is enabled.

To erase the configuration, click the **Erase** button.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See "Restoring the Default Configuration and Password" on page 8-7.

Upgrading the Router Software

	Tip: To ensure you are always using the latest firmware, enable the Firmware Upgrade Assistant feature so that the router will automatically detect a new version of the firmware on the Internet and alert you to its availability.

This screen appears at login unless you check Do Not Display This Message Again and click **Yes**.

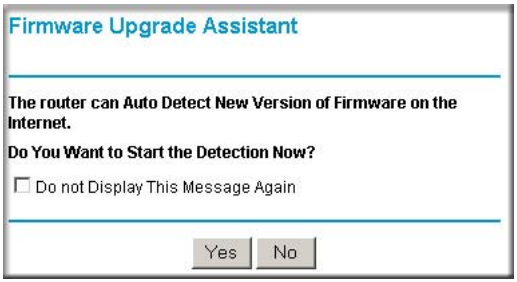


Figure 6-6

	Tip: Before upgrading the router software, use the router backup menu to save your configuration settings. A router upgrade may revert the router settings back to the factory defaults. If so, after completing the upgrade, you can restore your settings from the backup.

The routing software of the WNR834B router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR Web site. If the upgrade file is compressed (.ZIP file), you must first extract the file before sending it to the router. The upgrade file can be sent to the router using your browser.

	Note: The Web browser used to upload new firmware into the WNR834B router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 3.0 or above.

From the main menu of the browser interface, under the Maintenance heading, select the **Router Upgrade** link to display the menu shown below.

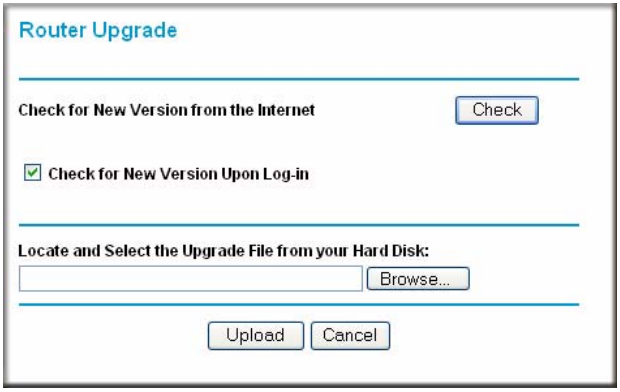


Figure 6-7

To upload new firmware:

1. Click the **Check** button to download and unzip (if the download file is a .zip file) the new software file from NETGEAR.
2. Click the **Browse** button and browse to the location of the upgrade file.
3. Click **Upload**.

⚠	**Warning:** When uploading software to the WNR834B router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your router will automatically restart. The upgrade process typically takes about one minute.

In some cases, you may need to reconfigure the router after upgrading.

Changing the Administrator Password

	Tip: Before changing the router password, use the router backup utility to save your configuration settings. If after changing the password, you forget the new password you assigned, you will have to reset the router back to the factory defaults to be able to log in using the default password of **password**. This means you will have to restore all the router configuration settings. If you ever have to reset the router back to the factory defaults, you can restore your settings from the backup.

The default password for the router's Web Configuration Manager is **password**. NETGEAR recommends that you change this password to a more secure password.

From the main menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown below.

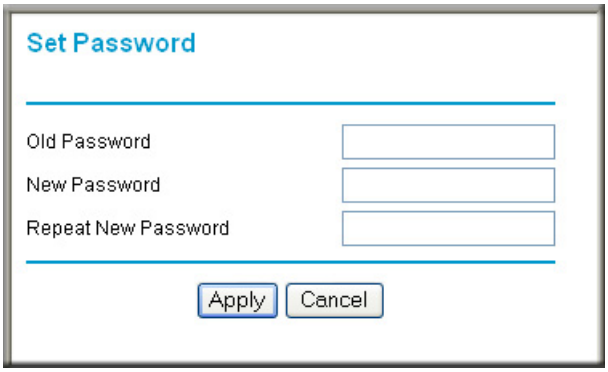


Figure 6-8

To change the password, first enter the old password, then enter the new password twice. Click **Apply**.

Chapter 7
Advanced Configuration of the Router

This chapter describes how to configure the advanced features of your RangeMax Next Wireless Router WNR834B. These features can be found under the Advanced heading in the main menu of the browser interface.

	Note: If you are unfamiliar with networking and routing, see "Wireless Communications" in Appendix B, to become more familiar with the terms and procedures used in this chapter.

Configuring Advanced Wireless Settings

Click on **Wireless Settings** under the Advanced Heading in the main menu to display the Advanced Wireless Settings screen:

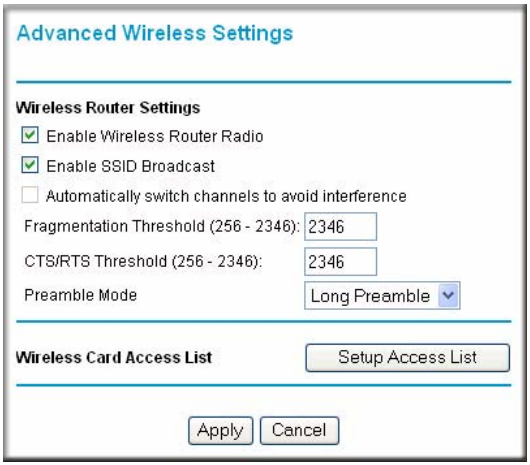


Figure 7-1

⚠	**Warning:** The Wireless Router is already configured with the optimum settings. Do not alter these settings unless directed by NETGEAR support. Incorrect settings may disable the Wireless Router unexpectedly.

Program the advanced wireless settings as follows:

- **Enable Wireless Router Radio**—the Wireless Router Radio of this router can be enabled or disabled to allow wireless access. The wireless icon on the front of the router displays the current status of the Wireless Router Radio to let you know if it is disabled or enabled. If enabled, wireless stations will be able to access the Internet. If disabled, wireless stations will not be able to access the Internet.
- **Enable SSID Broadcast**—if enabled, the Wireless Router SSID will broadcast its name (SSID) to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.
- **Automatically switch channels to avoid interference.** If enabled, the WNR834B router will periodically survey the wireless environment to ensure that it is using the clearest channel. If a clearer channel is available, it may automatically switch channels.

➡	**Note:** After the router switches channels, there may be a slight delay while your wireless computers reconnect to the router. If you want to avoid this possibility, leave this checkbox unselected.

- **Fragmentation Threshold, CTS/RTS Threshold, Preamble Mode**—these settings are reserved for wireless testing and advanced configuration only. Do not change these settings.
- **Wireless Card Access List**—by default, any wireless computer that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific computers based on their MAC addresses.

Wireless Card Access List

The Wireless Card Access Setup page displays a list of wireless computers that are allowed to connect to the router based on their MAC addresses. These wireless computers must also have the correct SSID and WEP settings configured on the Wireless Settings page to access the wireless network.

From the Advanced Wireless Settings menu, click the **Setup Access List** button to display the Wireless Access List menu:

Figure 7-2

Program the wireless card access list as follows:

1. Turn access control on:

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

b. Click the **Apply** button to save changes and return to the Wireless Settings page.

	Note: If Turn Access Control On is enabled and the Access Control List is blank; then no wireless computers will be able to connect to your wireless network.

2. Set Up The Access Control List:

a. Click the **Add** button to go to the Access Setup menu (see Figure 7-3). This menu displays a list of currently active wireless cards and their Ethernet MAC addresses.

b. If the desired computer appears in the list, you can click the radio button of that computer to capture its MAC address; otherwise, you can manually enter the MAC address of the authorized computer. The MAC address can usually be found on the bottom of the wireless device.

c. If no Device Name appears, you can type a descriptive name for the computer that you are adding.

d. When you have finished entering the MAC address, return to the Wireless Access List menu by clicking the **Add** button.

e. Repeat steps a - d for each wireless computer.

f. Click the **Turn Access Control On** box to enable Access Control.

g. Click the **Apply** button to save changes and return to the Wireless Settings page.

Wireless Card Access Setup

The Wireless Card Access Setup screen is invoked by clicking **Add** on the Wireless Card Access List menu (see "Wireless Card Access List" on page 7-3):

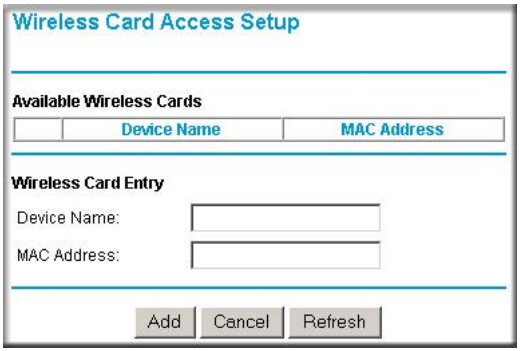


Figure 7-3

Program the Wireless Card Access Setup menu as follows:

- **Available Wireless Cards**—the Available Wireless Cards list displays any available wireless computers and their MAC addresses.

  If the wireless computer appears in the Available Wireless Cards list, you can click on the radio button of that computer to capture its MAC address. If your wireless computer is not displayed, make sure that the computer is configured correctly, and then click on the **Refresh** button to update the available list of wireless computers. If the wireless computer is still not displayed, then follow the instructions below on how to manually setup the wireless computer's MAC address.

- **Wireless Card Entry**—if no wireless computers appear in the Available Wireless Cards list, you can manually enter the Device Name and MAC address of the authorized wireless computer.

	Note: The MAC address is a twelve character key containing the characters 0-9, A-F only and separated by colons (for example., 00:09:AB:CD:EF:01) that can usually be found on the bottom of the wireless device.

Configuring Port Triggering and Port Forwarding

Port Triggering is an advanced feature that can be used to easily enable gaming and other Internet applications. Port Forwarding is typically used to enable similar functionality, but it is static and has some limitations.

	Note: If you use applications such as multi-player gaming, peer-to-peer connections, real time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable UPnP according to the instructions at "Using Universal Plug and Play (UPnP)" on page 7-22.

Port Triggering opens an incoming port temporarily and does not require the server on the Internet to track your IP address if it is changed by DHCP, for example.

Port Triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and triggers the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

Using the Port Triggering page, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games (like Quake III), or to use Internet applications (like CUseeMe).

Port forwarding is designed for FTP, Web Server or other server-based services. Once port forwarding is set up, requests from the Internet will be forwarded to the proper server. Port triggering will only allow requests from the Internet after a designated port is 'triggered'. Port triggering applies to chat and Internet games.

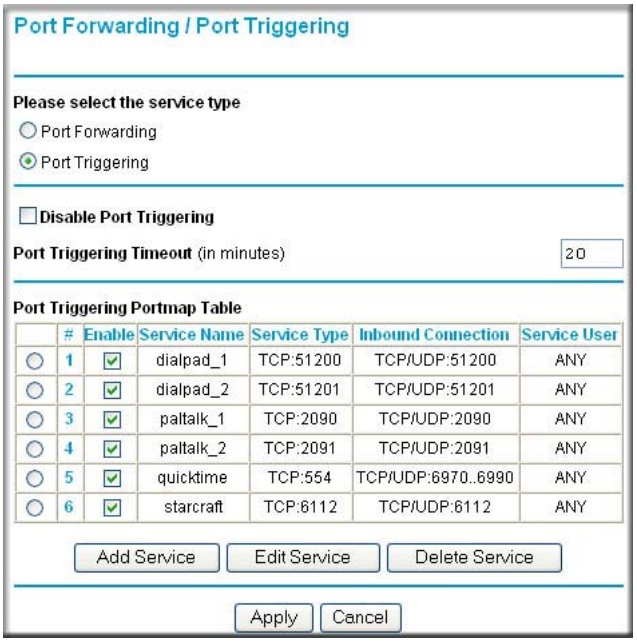


Figure 7-4

	Note: If the Disable Port Triggering box is checked after configuring port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it will not be used.

- **Port Triggering Timeout**—Enter a value up to 9999 minutes. The Port Triggering Timeout value controls the inactivity timer for the designated inbound port(s). The inbound port(s) close when the inactivity timer expires.
- **For Internet Games or Applications**—Before starting, you need to know which service, application or game you will be configuring. Also, you need to have the outbound port (triggering port) address for this game or application.

Follow these steps to set up a computer to play Internet games or use Internet applications:

1. Select **Port Forwarding / Port Triggering** from the Advanced section of the main menu.
2. Select the service type by clicking the **Port Triggering** radio button. The Port Triggering screen is displayed as shown in Figure 7-4.
3. Click **Add Service**.

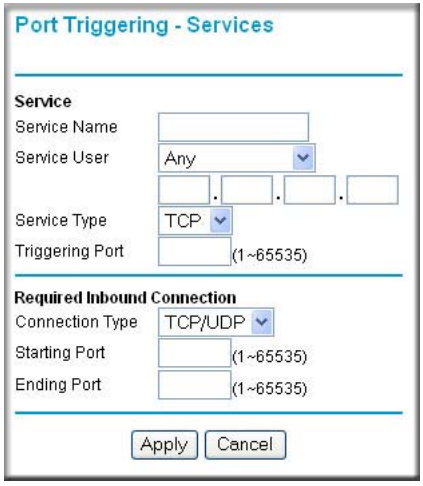


Figure 7-5

4. Enter a service name in the Service Name box.
5. Under Service User, select **Any** (default) to allow this service to be used by everyone in your network. Otherwise, select **Single address** and enter the IP address of one computer to restrict the service to a particular computer.
6. Select the Service Type.
7. Enter the outbound port number in **Triggering Port** box.
8. Enter the inbound connection port information such as Connection Type, Starting Port and Ending Port boxes. This information can be obtained from the game or applications manual or the product's support Web site.
9. Click **Apply** to save your changes.

Configuring Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make a local server (for example, a Web server or game server) visible and available to the Internet. This is done using the Port Forwarding menu.

Use the Port Forwarding menu to configure the router to forward incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the WAN Setup menu as discussed in "Configuring the WAN Setup Options" on page 7-11.

Before starting, you need to determine which type of service, application or game you will provide, and the IP address of the computer that will provide the service. Be sure the computer's IP address never changes.

Note: To assure that the same computer always has the same IP address, use the reserved IP address feature of your WNR834B router. See "Using Address Reservation" on page 7-15 for instructions on how to use reserved IP addresses.

To configure port forwarding to a local server:

1. From the main menu of the browser interface, under Advanced, click on **Port Forwarding / Port Triggering** to view the port forwarding menu, shown below.

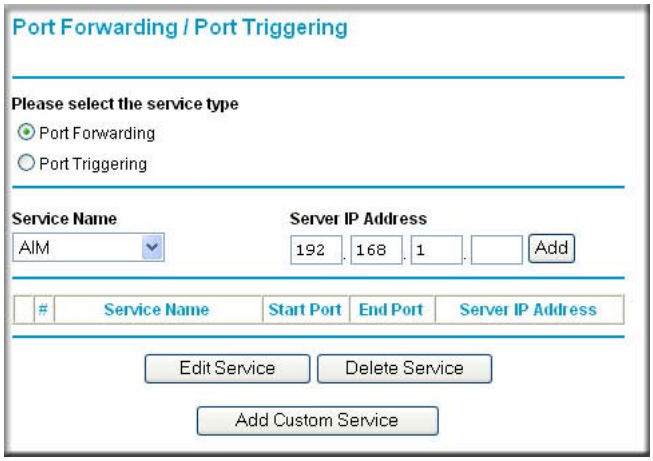


Figure 7-6

2. From the Service Name box, select the service or game that you will host on your network. If the service does not appear in the list, see the following section, Adding a Custom Service.
3. Enter the IP address of the local server in the corresponding Server IP Address box.
4. Click the **Add** button.

Adding a Custom Service

To define a service, game or application that does not appear in the Service Name list, you must determine what port numbers the service will use. For this information, you may need to contact the manufacturer of the program that you wish to use. When you have the port number information, follow these steps:

1. Select **Port Forwarding / Port Triggering** from the Advanced Section of the main menu, as described in the preceding section.
2. Click the **Add Custom Service** button.

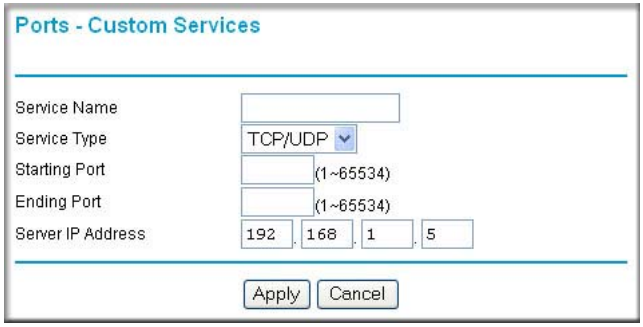


Figure 7-7

3. Type the service name in the Service Name box.
4. Type the beginning port number in the Starting Port box.
   - If the application uses only a single port; type the same port number in the Ending Port box.
   - If the application uses a range of ports; type the ending port number of the range in the Ending Port box.
5. Type the IP address of the computer in the Server IP Address box.
6. Click **Apply** to save your changes.

Editing or Deleting a Port Forwarding Entry

To edit or delete a Port Forwarding entry, follow these steps.

1. In the table, select the button next to the service name.
2. Click the **Edit Service** or **Delete Service** button.

Local Web and FTP Server Example

If a local computer with a private IP address of 192.168.1.33 acts as a Web and FTP server, configure the Ports menu to forward HTTP (port 80) and FTP (port 21) to local address 192.168.1.33

In order for a remote user to access this server from the Internet, the remote user must know the IP address that has been assigned by your ISP. If this address is 172.16.1.23, for example, an Internet user can access your Web server by directing the browser to http://172.16.1.23. The assigned IP address can be found in the Router Status Menu, where it is shown as the WAN IP Address.

Some considerations for this application are:

- If your account’s IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires.
- If the IP address of the local computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, you can manually configure the computer to use a fixed address.
- Local computers must access the local server using the computers’ local LAN address (192.168.1.33 in this example). Attempts by local computers to access the server using the external IP address (172.16.1.23 in this example) will fail.

Multiple Computers for Internet Gaming

To set up an additional computer to play Age of Empire or Quake III:

1. Click the button of an unused port in the table.
2. Select the game again from the Services/Games list.
3. Change the beginning port number in the Start Port box.
   For these games, use the supplied number in the default list and add +1 for each additional computer. For example, if you have already configured one computer to play Hexen II (using port 26900), the second computer's port number would be 26901, and the third computer would be 26902.
4. Type the same port number in the End Port box that you typed in the Start Port box.

5. Type the IP address of the additional computer in the Server IP Address box.
6. Click **Apply**.

Some online games and videoconferencing applications are incompatible with NAT. The WNR834B router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default in the Port Forwarding / Port Triggering Menu. If one local computer acts as a game or videoconferencing host, enter its IP address as the default.

Configuring the WAN Setup Options

The WAN Setup options let you configure a DMZ server, change the MTU size and enable the wireless router to respond to a Ping on the WAN port. These options are discussed below.

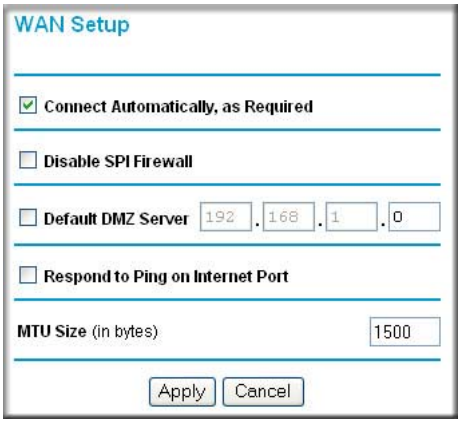


Figure 7-8

Connecting Automatically, as Required

Normally, this option should be checked to enable it. An Internet connection will be made automatically after each timeout, whenever Internet-bound traffic is detected. This provides connection on demand and is potentially cost-saving, in some regions of Europe for example, where Internet services charge by the minute.

If disabled, you must connect manually, using the "Connection Status" button on the Router Status screen. This manual connection will stay up all the time without timeouts.

Disabling the SPI Firewall

The SPI (Stateful Inspection) Firewall protects your LAN against Denial of Service attacks. This should only be disabled in special circumstances.

Setting Up a Default DMZ Server

The default DMZ server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The router is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local computer can run the application properly if that computer's IP address is entered as the default DMZ server.

	Note: DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall, and is exposed to exploits from the Internet. If compromised, the DMZ server can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Port Forwarding / Port Triggering menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The WAN Setup menu lets you configure a Default DMZ Server.

To assign a computer or server to be a Default DMZ server, follow these steps:

1. Click **WAN Setup** link in the Advanced section of the main menu.
2. Type the IP address for that server. To remove the default DMZ server, replace the IP address numbers with all zeros.
3. Click **Apply**.

Responding to a Ping on the Internet WAN Port

If you want the router to respond to a 'ping' from the Internet, click the **Respond to Ping on Internet WAN Port** check box. This should only be used as a diagnostic tool, since it allows your router to be discovered. Do not check this box unless you have a specific reason to do so.

Setting the MTU Size

The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, 1492 Bytes for PPPoE connections, or 1436 for PPTP connections. For some ISPs you may need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Any packets sent through the router that are larger than the configured MTU size are repackaged into smaller packets to meet the MTU requirement. To change the MTU size:

1. Under MTU Size, enter a new size between 64 and 1500.
2. Click **Apply** to save the new configuration.

Using the LAN IP Setup Options

Another category under the Advanced heading is LAN IP Setup. This menu allows configuration of LAN IP services such as DHCP and RIP. From the main menu of the browser interface, under Advanced, click on **LAN IP Setup** to view the LAN IP Setup menu, shown below.

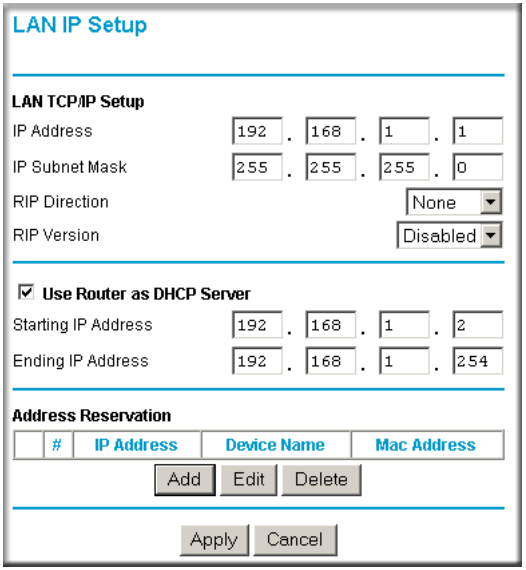


Figure 7-9

Configuring LAN TCP/IP Setup Parameters

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

- LAN IP address—192.168.1.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable for most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN IP parameters are:

- IP Address
  This is the LAN IP address of the router.
- IP Subnet Mask
  This is the LAN Subnet Mask of the 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 router.
- RIP Direction
  RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.
  - When set to Both or Out Only, the router broadcasts its routing table periodically.
  - When set to Both or In Only, the router incorporates the RIP information that it receives.
  - When set to None, the 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 router sends. (It recognizes both formats when receiving.) By default, this is set for 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. RIP-2B uses subnet broadcasting.

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

Using the Router as a DHCP server

By default, the router functions as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. The router assigns IP addresses to the attached computers from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See "Wireless Communications" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.254, although you may wish 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 menu; otherwise, the router's LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu)

To select another device on your network as the DHCP server, or to manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box. Otherwise, leave it checked.

Using Address Reservation

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

To reserve an IP address:

1. Click the **Add** button.
2. In the IP Address box, type the IP address to assign to the computer or server. (choose an IP address from the router's LAN subnet, such as 192.168.1.x)

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

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

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

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

To edit or delete a reserved address entry:

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

Using a Dynamic DNS Service

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 do 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, which 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.

	Note: If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the dynamic DNS service will not work because private addresses are not routed on the Internet.

The router contains a client that can connect to many popular dynamic DNS services. You can select one of these services and obtain an account with them. Then, 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.

From the main menu of the browser interface, under Advanced, click on **Dynamic DNS**.

Figure 7-10

To configure Dynamic DNS:

1. Register for an account with one of the dynamic DNS service providers whose names appear in the **Select Service Provider** box. For example, for dyndns.org, go to **www.dyndns.org**.
2. Select the **Use a Dynamic DNS Service** check box.
3. Select the name of your dynamic DNS Service Provider.
4. Type the Host Name (or domain name) that your dynamic DNS service provider gave you.
5. Type the User Name for your dynamic DNS account.
6. Type the Password (or key) for your dynamic DNS account.
7. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the **Use wildcards** check box to activate this feature.
   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
8. Click **Apply** to save your configuration.

Configuring 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.

From the main menu of the browser interface, under Advanced, click on **Static Routes** to view the Static Routes menu, shown below.

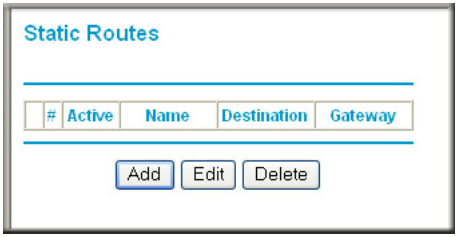


Figure 7-11

To add or edit a Static Route:

1. Click the **Add** button to open the Add/Edit Menu, shown below.

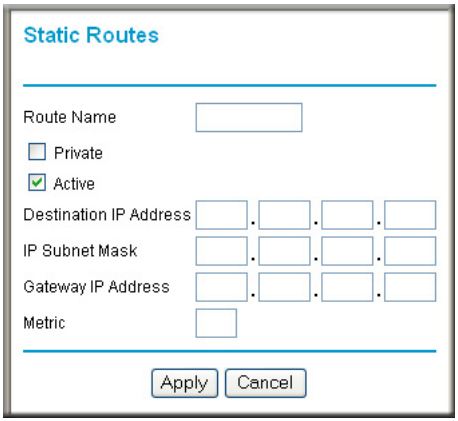


Figure 7-12

2. Type a route name for this static route in the Route Name box.
(This is for identification purposes only.)

3. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Select **Active** to make this route effective.
5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type 255.255.255.255.
7. Type the Gateway IP Address, which must be a router on the same LAN segment as the WNR834B.
8. Type a number between 1 and 15 as the Metric value.
   This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click **Apply** to have the static route entered into the table.

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

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.1.100.
- Your company's network address is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.1.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. The static route would look like Figure 7-12.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.1.100.
- A Metric value of 1 will work since the ISDN router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your WNR834B router.

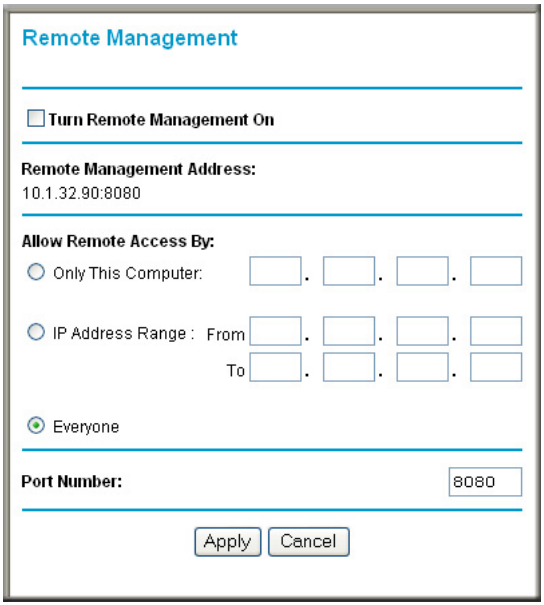


Figure 7-13

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

To configure your router for Remote Management:

1. Select the **Turn Remote Management On** check box.
2. Specify what external addresses will be allowed to access the router’s remote management.

	Note: For enhanced security, restrict access to as few external IP addresses as practical.

a. To allow access from any IP address on the Internet, select **Everyone**.

b. 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.

c. To allow access from a single IP address on the Internet, select **Only this computer**. Enter the IP address that will be allowed access.

3. Specify the Port Number for accessing the management interface.

Web browser access normally uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote management Web interface. 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.

4. Click **Apply** to have your changes take effect.

Note: When accessing your router from the Internet, type your router's WAN IP address into your browser's Address (in Internet Explorer) or Location (in Netscape) box, 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, then enter http://134.177.0.123:8080 in your browser.

Using Universal Plug and Play (UPnP)

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.

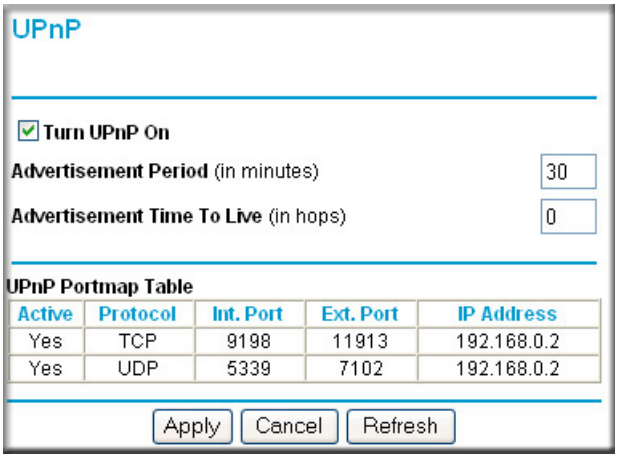


Figure 7-14

From the main menu of the browser interface, under Advanced, click on **UPnP**. Set up UPnP according to the guidelines below.

Turn UPnP On—UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.

	Note: If you use applications such as multi-player gaming, peer-to-peer connections, real time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should enable UPnP.

Advertisement Period—the Advertisement Period is how often the router will broadcast 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 may compromise the freshness of the device status but can significantly reduce network traffic.

Advertisement Time To Live—the time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is 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 may 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 router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is open and if that port is still active for each IP address.

Chapter 8
Troubleshooting

This chapter gives information about troubleshooting your RangeMax Next Wireless Router WNR834B. After each problem description, instructions are provided to help you diagnose and solve the problem.

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 that:
   - **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 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 connected to a 10 Mbps device, the light is amber.

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

Power Light 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 properly connected to a functioning power outlet.
- Check that you are using the 12V DC 1A power adapter that NETGEAR supplies 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 turns 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:

- Cycle the power 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. The procedure is explained in "Restoring the Default Configuration and Password" on page 8-7.

If the error persists, you might have a hardware problem and should contact technical support.

LAN or WAN Port Lights Not On

If either the LAN lights or Internet light do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
  - When connecting the 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.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration interface 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 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, see "Preparing a Computer for Network Access" in Appendix B to configure your computer.

	Note: If your computer's IP address is shown as 169.254.x.x: Recent versions of Windows and Mac OS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in subnet 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.

- If your router's IP address has been changed and you don't 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 8-7.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when 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 menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes may have occurred, but the Web browser may 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 the Maintenance heading, 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 may 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 five 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 may be one of the following:

- Your ISP may 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, you may have incorrectly set the login name and password.
- Your ISP may check for your computer's host name.
  Assign the computer Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:

Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

OR

Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu. For more information, see "How to Manually Configure Your Internet Connection" on page 3-6.

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

- Your computer may 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 will provide 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 as described in "Preparing a Computer for Network Access" in Appendix B. Alternatively, you may configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer may 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 "Preparing a Computer for Network Access" in Appendix B.

Troubleshooting a TCP/IP Network Using a 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. Troubleshooting a TCP/IP network is made very easy 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 on 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 LED is on. If the LED is off, follow the instructions in "LAN or WAN Port Lights Not On" on page 8-2.
     - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
   - Wrong network configuration
     - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your 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. From the Windows run menu, 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 like those shown 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 will not be visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in "Preparing a Computer for Network Access" in Appendix B.
- — Check to see that the network address of your computer (the portion of the IP address specified by the subnet mask) 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 menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by only allowing 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 to “clone” or “spoof” the MAC address from the authorized computer. For more information, see “How to Manually Configure Your Internet Connection” on page 3-6.

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:

- Use the Erase function of the router (see “Erasing the Configuration” on page 6-6).
- Use the Default Reset 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 without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button until the test light blinks on (about 10 seconds).

2. Release the Default Reset 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 may 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 menu in the Content Filtering section displays the current date and time of day. The WNR834B router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five 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 menu, check or clear the box marked “Adjust for Daylight Savings Time”.

Appendix A
Technical Specifications

This appendix provides technical specifications for the RangeMax Next Wireless Router WNR834B.

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPP over Ethernet (PPPoE) PPtP, Bigpond, Dynamic DNS, and UPnP
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):	5V DC @ 1A output
Physical Specifications	
Dimensions:	286 x 147 x 957mm (1.1 x 5.8x 3.8in.)
Weight:	0.20 kg (0.45 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 VCCI Class B EN 550 22/24 (CISPR 22/24) 60950 (CS LVD) Class B MIC
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45

WAN:	10BASE-T or 100BASE-Tx, RJ-45
Wireless	
Radio Data Rates	1, 2, 5.5, 6, 6.5, 9, 11, 12, 13.5, 18, 19.5, 24, 26, 27, 36, 39, 40, 40.5, 48, 52, 54, 58.5, 65, 72, 80, 81, 84, 96, 104, 108, 117, 120, 121.5, 130, 135, 144, 160, 168, 192, 216, 240, and 270 Mbps
Frequency	2.4-2.5 Ghz
Data Encoding:	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes.
Operating Frequency Ranges:	2.412~2.462 GHz (US) 2.412~2.472 GHz (Japan) 2.412~2.472 GHz (Europe ETSI)
802.11 Security:	40-bit (also called 64-bit) and 128-bit WEP, WPA-PSK and WPA2-PSK.

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.

Document	Link
Internet Networking and TCP/IP Addressing	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN)	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary	http://documentation.netgear.com/reference/enu/glossary/index.htm