N 150 Wireless Router WNR1000 v2h2 User Manual

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

August 2010
v1.0

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 at *http://www.netgear.com/support*.

Setup documentation is available on the CD, on the support website, and on the documentation website. When the wireless router is connected to the Internet, click the Knowledge Base or the Documentation link under Web Support on the main menu to view support information.

Trademarks

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

Statement of Conditions

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

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

Certificate of the Manufacturer/Importer

It is hereby certified that the N 150 Wireless Router WNR1000 v2h2 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.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das N 150 Wireless Router WNR1000 v2h2 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.

Regulatory Compliance Information

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

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

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN 60950-1: 2001
  Safety of information technology equipment
- EN 300 328 V1.7.1 (2006-10)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 489-17 V1.2.1 (2002-08) and EN 301 489-1 V1.4.1 (2002-08)
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries under the following conditions and/or with the following restrictions:

- In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.
- This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

Europe – Declaration of Conformity in Languages of the European Community

cs Česky [Czech]	*[NETGEAR Inc.]* tímto prohlašuje, že tento *[WNR1000 v2h2]* je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
da Dansk [Danish]	Undertegnede *[NETGEAR Inc.]* erklærer herved, at følgende udstyr *[WNR1000v2h2]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt *[NETGEAR Inc.]*, dass sich das Gerät *[WNR1000 v2h2]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab *[NETGEAR Inc.]* seadme *[WNR1000 v2h2]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, *[NETGEAR Inc.]*, declares that this *[WNR1000 v2h2]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

es Español [Spanish]	Por medio de la presente *[NETGEAR Inc.]* declara que el *[WNR1000 v2h2]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[NETGEAR Inc.]* ΔΗΛΩΝΕΙ ΟΤΙ *[WNR1000 v2h2]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente *[NETGEAR Inc.]* déclare que l'appareil *[WNR1000 v2h2]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente *[NETGEAR Inc.]* dichiara che questo *[WNR1000 v2h2]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[NETGEAR Inc.]* deklarē, ka *[WNR1000 v2h2]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[NETGEAR Inc.]* deklaruoja, kad šis *[WNR1000 v2h2]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart *[NETGEAR Inc.].* dat het toestel *[WNR1000 v2h2]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, *[NETGEAR Inc.]*, jiddikjara li dan *[WNR1000 v2h2]* jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, *[NETGEAR Inc.]* nyilatkozom, hogy a *[WNR1000 v2h2]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[NETGEAR Inc.]* oświadcza, że *[WNR1000 v2h2]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	*[NETGEAR Inc.]* declara que este *[WNR1000 v2h2]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	*[NETGEAR Inc.]* izjavlja, da je ta *[WNR1000 v2h2]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[NETGEAR Inc.]* týmto vyhlasuje, _e *[WNR1000 v2h2]* spĺňa základné po_iadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	*[NETGEAR Inc.]* vakuuttaa täten että *[WNR1000 v2h2]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar *[NETGEAR Inc.]* att denna *[WNR1000 v2h2]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

FCC Requirements for Operation in the United States

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.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

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.

FCC Information to User

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

FCC Guidelines for Human Exposure

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

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

FCC Declaration Of Conformity

We NETGEAR, Inc., 4500 Great America Parkway, Santa Clara, CA 95054, declare under our sole responsibility that the model N 150 Wireless Router WNR1000 v2h2 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

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

FCC Radio Frequency Interference Warnings & Instructions

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

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

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

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE
Radiation Exposure Statement:

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

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.

Product and Publication Details

Model Number:	WNR1000 v2h2
Publication Date:	August 2010
Product Family:	Wireless Router
Product Name:	**N 150 Wireless Router WNR1000 v2h2**
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10546-01

Contents

About This Manual

Conventions, Formats, and Scope xi
How to Use This Manual xii
How to Print This Manual xiii
Revision History xiii

Chapter 1
Configuring Basic Connectivity

Using the Setup Manual 1-1
Logging In To Your Wireless Router 1-2
Selecting a Language for Your Screen Display 1-4
Configuring Your Internet Settings Using the Setup Wizard 1-6
Viewing and Configuring Basic Internet Settings 1-6
Your Internet Connection Does Not Require a Login 1-7
Your Internet Connection Does Require a Login 1-9
Setting Up and Testing Basic Wireless Connectivity 1-11

Chapter 2
Safeguarding Your Network

Choosing Appropriate Wireless Security 2-1
Recording Basic Wireless Settings Setup Information 2-5
Changing Wireless Security Settings 2-6
Viewing Basic Wireless Settings 2-6
Configuring WEP Wireless Security 2-8
Configuring WPA-PSK and WPA2-PSK Wireless Security 2-10
Viewing Advanced Wireless Settings 2-11
Using Push 'N' Connect (Wi-Fi Protected Setup) 2-13
Push Button Configuration 2-13
Security PIN Entry 2-15
Configuring the WPS Settings 2-16
Connecting Additional Wireless Client Devices after WPS Setup 2-17

Restricting Wireless Access by MAC Address 2-18
Changing the Administrator Password 2-20
Backing Up Your Configuration 2-21
Understanding Your Firewall 2-22

Chapter 3
Restricting Access From Your Network

Content Filtering Overview 3-1
Blocking Access to Internet Sites 3-1
Blocking Access to Internet Services 3-3
Blocking Services by IP Address Range 3-5
Scheduling Blocking 3-5
Viewing Logs of Web Access or Attempted Web Access 3-6
Configuring E-mail Alert and Web Access Log Notifications 3-7
Setting the Time Zone 3-8

Chapter 4
Customizing Your Network Settings

Using the LAN IP Setup Options 4-1
Configuring a Device Name 4-2
Configuring LAN TCP/IP Setup Parameters 4-2
Using the Router as a DHCP Server 4-3
Using Address Reservation 4-4
Using a Dynamic DNS Service 4-5
Configuring the WAN Setup Options 4-6
Disabling the SPI Firewall 4-6
Setting Up a Default DMZ Server 4-7
Responding to a Ping on the Internet (WAN) Port 4-7
Setting the MTU Size 4-8
Configuring NAT Filtering 4-8
Configuring Static Routes 4-8

Chapter 5
Fine-Tuning Your Network

Allowing Inbound Connections to Your Network 5-1

How Your Computer Accesses a Remote Computer through Your Router 5-2

How Port Triggering Changes the Communication Process 5-3

How Port Forwarding Changes the Communication Process 5-5

How Port Forwarding Differs from Port Triggering 5-6

Configuring Port Forwarding to Local Servers 5-6

Adding a Custom Service 5-7

Editing or Deleting a Port Forwarding Entry 5-8

Configuring Port Triggering 5-9

Using Universal Plug and Play 5-12

Optimizing Wireless Performance 5-14

Changing the MTU Size 5-15

Overview of Home and Small Office Networking Technologies 5-16

Assessing Your Speed Requirements 5-17

Chapter 6
Using Network Monitoring Tools

Viewing Wireless Router Status Information 6-2

Viewing a List of Attached Devices 6-7

Managing the Configuration File 6-7

Backing Up and Restoring the Configuration 6-8

Erasing the Configuration 6-8

Updating the Router Firmware 6-9

Checking for New Firmware in the Router Upgrade Screen 6-9

Updating Manually to New Router Firmware 6-10

Enabling Remote Management Access 6-12

Traffic Meter 6-14

Chapter 7
Troubleshooting

Quick Tips 7-1

Troubleshooting Basic Functions 7-2

Login Problems 7-5

Checking the Internet Service Connection 7-6

Obtaining an Internet IP Address 7-6

Troubleshooting PPPoE 7-7

Troubleshooting Internet Browsing 7-8

Troubleshooting Your Network Using the Ping Utility 7-8

Testing the LAN Path to Your Router 7-9

Testing the Path from Your Computer to a Remote Device 7-10

Problems with Date and Time 7-10

Problems with Wireless Adapter Connections 7-11

Restoring the Default Configuration and Password 7-12

Appendix A
Technical Specifications

Default Configuration Settings A-1

General Specifications A-3

Appendix B
Related Documents

Index

About This Manual

The user manual provides information for configuring the features of the NETGEAR®N 150 Wireless Router WNR1000 v2h2 beyond initial configuration settings. Initial configuration instructions can be found in the *NETGEAR Wireless Router Setup Manual*. You should have basic to intermediate computer and Internet skills.

Conventions, Formats, and Scope

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

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

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

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

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

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

Warning: Ignoring this type of note might result in a malfunction or damage to the equipment, a breach of security, or a loss of data.

Danger: This is a safety warning. Failure to take heed of this notice might result in personal injury or death.

- **Scope**. This manual is written for the WNR1000 v2h2 router according to these specifications:

Product Version	N 150 Wireless Router WNR1000 v2h2
Manual Publication Date	August 2010

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

Note: Product updates are available on the NETGEAR, Inc. website at *http://www.netgear.com/support*.

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print This Manual

To print this manual, 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*.

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

Revision History

NETGEAR, Inc. is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the WNR1000v2 router was introduced.

Table 2-1. Publication Revision History

Part Number	Version Number	Date	Description
202-10546-01	v1.0	August 2010	First publication.

Chapter 1
Configuring Basic Connectivity

This chapter describes the settings for your Internet connection and your wireless local area network (LAN) connection. When you perform the initial configuration of your wireless router using the *Resource CD* as described in the *NETGEAR Wireless Router Setup Manual,* these settings are specified automatically for you. This chapter provides further details about these connectivity settings, as well as instructions on how to log in to the router for further configuration.

➡	**Note:** NETGEAR recommends using the Smart Wizard™ on the *Resource CD* for initial configuration, as described in the *NETGEAR Wireless Router Setup Manual*.

This chapter includes the following sections:

- "Using the Setup Manual" on page 1-1
- "Logging In To Your Wireless Router" on page 1-2
- "Selecting a Language for Your Screen Display" on page 1-4
- "Configuring Your Internet Settings Using the Setup Wizard" on page 1-6
- "Viewing and Configuring Basic Internet Settings" on page 1-6
- "Setting Up and Testing Basic Wireless Connectivity" on page 1-11

Using the Setup Manual

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

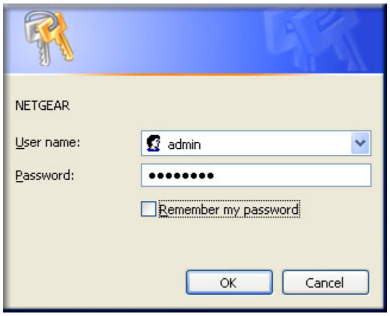
For installation instructions in a language other than English, refer to the language options on the *Resource CD*.

Logging In To Your Wireless Router

When the wireless router is connected to your network, you can access and configure the router using your browser. The Default Access login information is printed on the bottom label of your router.

To access the router:

1. Connect to the wireless router by typing **http://www.routerlogin.net** in the address field of your browser, and then press **Enter**. A login window displays.



NETGEAR

User name: admin

Password: ●●●●●●●●●

□ Remember my password

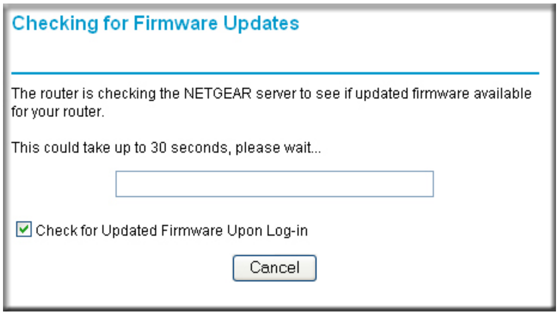
Figure 1-1

	Tip: You can connect to the wireless router by typing either of these URLs in the address field of your browser, and then pressing **Enter**: • **http://www.routerlogin.net** • **http://www.routerlogin.com** If these URLs do not work, you must type the IP address of the router, for example, **http://192.168.1.1**.

2. Enter **admin** for the router user name and your password (or the default, **password**).

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

- The Checking for Firmware Updates screen appears unless you previously cleared the **Check for Updated Firmware Upon Log-in** check box.



Checking for Firmware Updates

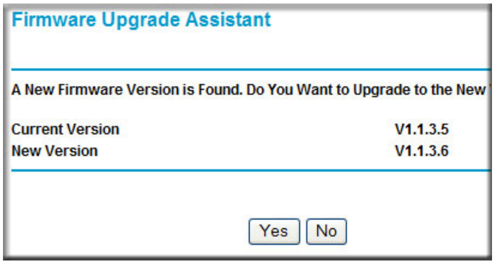
The router is checking the NETGEAR server to see if updated firmware available for your router.

This could take up to 30 seconds, please wait...

☑ Check for Updated Firmware Upon Log-in

Figure 1-2

This message displays if the router discovers that new firmware is available. (If no new firmware is available, the router will proceed to the router status screen.)



Firmware Upgrade Assistant

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

Current Version	V1.1.3.5
New Version	V1.1.3.6

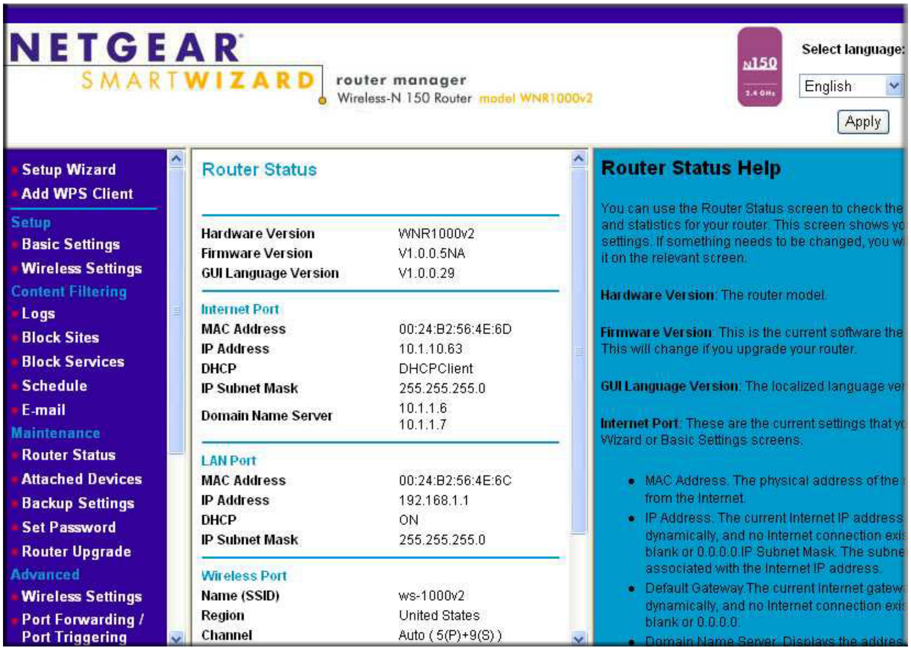
Figure 1-3

- To automatically update to the new firmware, click **Yes** to allow the router to download and install the new firmware file from NETGEAR.

⚠	**Warning:** When uploading firmware to the WNR1000v2 router, ***do not*** interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

The update process typically takes about 1 minute. When the upload is complete, your router automatically restarts.

3. If there is no new firmware, the login will take you to the Router Status screen displayed here.



Router Status

Hardware Version	WNR1000v2
Firmware Version	V1.0.0.5NA
GUI Language Version	V1.0.0.29
Internet Port	
MAC Address	00:24:B2:56:4E:6D
IP Address	10.1.10.63
DHCP	DHCPClient
IP Subnet Mask	255.255.255.0
Domain Name Server	10.1.1.6 10.1.1.7
LAN Port	
MAC Address	00:24:B2:56:4E:6C
IP Address	192.168.1.1
DHCP	ON
IP Subnet Mask	255.255.255.0
Wireless Port	
Name (SSID)	ws-1000v2
Region	United States
Channel	Auto (5(P)+9(S))

Router Status Help

You can use the Router Status screen to check the and statistics for your router. This screen shows yo settings. If something needs to be changed, you wi it on the relevant screen.

Hardware Version: The router model.

Firmware Version: This is the current software the This will change if you upgrade your router.

GUI Language Version: The localized language ver

Internet Port: These are the current settings that yo Wizard or Basic Settings screens.

- MAC Address. The physical address of the from the Internet.
- IP Address. The current Internet IP address dynamically, and no Internet connection exis blank or 0.0.0.0.IP Subnet Mask. The subne associated with the Internet IP address.
- Default Gateway.The current Internet gatew dynamically, and no Internet connection exis blank or 0.0.0.0.
- Domain Name Server. Displays the addres

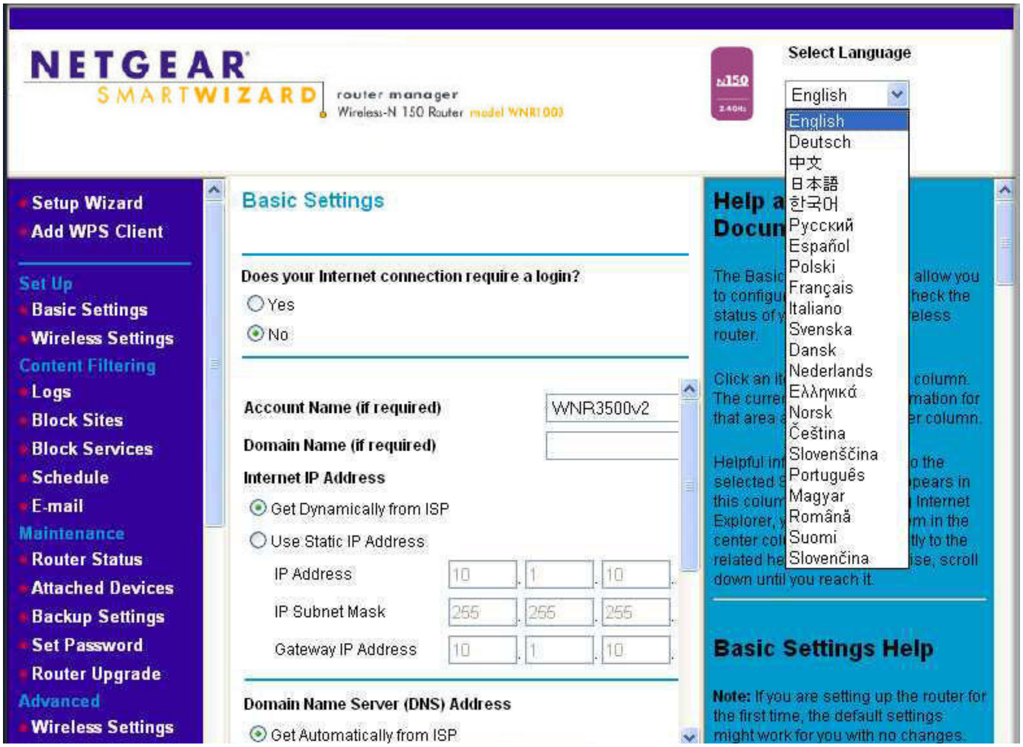
Figure 1-4

If the wireless router is connected to the Internet, you can select **Knowledge Base** or **Documentation** under Web Support in the main menu to view support information or the documentation for the wireless router.

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

Selecting a Language for Your Screen Display

Using the Select Language drop-down menu, located in the upper right corner of the Router Manager screen, you can display the router manager screens in any of languages shown in Figure 1-5:



Basic Settings

Does your Internet connection require a login?
○ Yes
● No

Account Name (if required) WNR3500v2
Domain Name (if required)
Internet IP Address
● Get Dynamically from ISP
○ Use Static IP Address
IP Address 10 . 1 . 10 .
IP Subnet Mask 255 . 255 . 255 .
Gateway IP Address 10 . 1 . 10 .

Domain Name Server (DNS) Address
● Get Automatically from ISP

Note: If you are setting up the router for the first time, the default settings might work for you with no changes.

Figure 1-5

The language is set to English by default. The default language is always stored in memory. When you select a language other than the default, that language as well as English is stored in memory. The additional language stored is the most recently selected. For example, if you select Deutsch, German and English will be stored. If you next select Chinese, Chinese and English will be stored.

To specify a language to be used on your router manager screens, do the following:

1. Expand the list and select the language you want.
2. Click **Apply**.

The language you select is then downloaded and displayed in the language selection box, and your screen display will be in the selected language.

> **Note:** You can select from the entire list of supported languages only when the router is connected to the Internet. When the router is not connected to the Internet, you can select one of the stored languages only.

Configuring Your Internet Settings Using the Setup Wizard

You can manually configure your Internet connection using the Basic Settings screen, or you can allow the Setup Wizard to determine your Internet Service Provider (ISP) configuration.

The Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

To use the Setup Wizard to assist with configuration or to verify the Internet connection settings:

1. Select **Setup Wizard** from the top of the main menu.
2. Click **Next** to proceed. Enter your ISP settings, as needed.
3. At the end of the Setup Wizard, click **Test** to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 7, “Troubleshooting.”

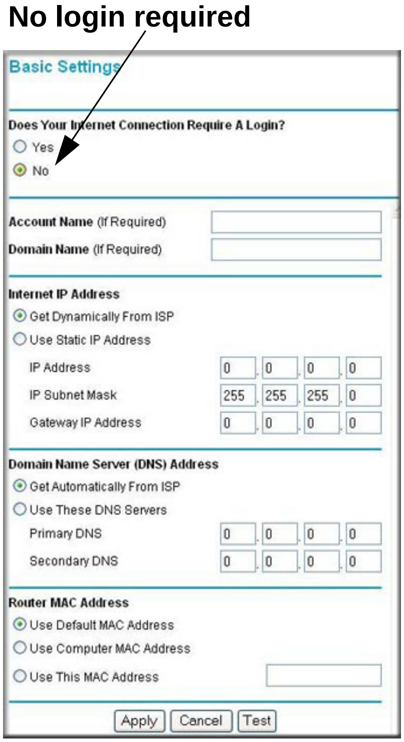
Viewing and Configuring Basic Internet Settings

Settings related to your Internet service are specified in the Basic Settings screen. Select **Basic Settings** under Setup in the main menu.

The content you see in the Basic Settings screen depends on whether your ISP requires that you log in with a user name and password for Internet access.

Your Internet Connection *Does Not* Require a Login

If no login is required by your ISP, the following settings appear in the Basic Settings screen.



No login required

Basic Settings

Does Your Internet Connection Require A Login?

○ Yes

● No

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

● Get Dynamically From ISP

○ Use Static IP Address

IP Address 0 . 0 . 0 . 0

IP Subnet Mask 255 . 255 . 255 . 0

Gateway IP Address 0 . 0 . 0 . 0

Domain Name Server (DNS) Address

● Get Automatically From ISP

○ Use These DNS Servers

Primary DNS 0 . 0 . 0 . 0

Secondary DNS 0 . 0 . 0 . 0

Router MAC Address

● Use Default MAC Address

○ Use Computer MAC Address

○ Use This MAC Address

Figure 1-6

- **Account Name** (might also be called Host Name). The account name is provided to the ISP during a DHCP request from your router. In most cases, this setting is not required, but some ISPs require it for access to ISP services such as mail or news servers.
- **Domain Name**. The domain name is provided by your router to computers on your LAN when the computers request DHCP settings from your router. In most cases, this settings is not required.
- **Internet IP Address**. Determines how your router obtains an IP address for Internet access.
  - If your ISP assigns an IP address dynamically (by DHCP), select **Get Dynamically From ISP**.

- 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 subnet mask and the gateway IP address. The gateway is the ISP's router to which your router will connect.

- **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 or change a DNS address, restart the computers on your network so that these settings take effect.

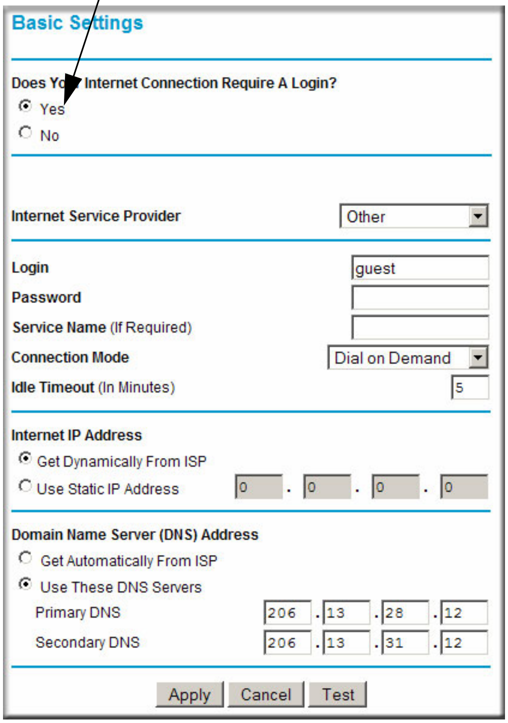
- **Router MAC Address**. This section determines the Ethernet MAC address that the router will use on the Internet port. Typically, you would leave **Use Default Address** selected. However, some ISPs (especially cable modem providers) register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They then accept only traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by "cloning" or "spoofing" its MAC address.

  To change the MAC address, select one of the following methods:

  - 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.
  - Select **Use This MAC Address**, and enter it here.

Your Internet Connection *Does* Require a Login

If a login is required by your ISP, the following settings appear in the Basic Settings screen:



Login required

Basic Settings

Does Your Internet Connection Require A Login?
● Yes
○ No

Internet Service Provider: Other

Login: guest
Password:
Service Name (If Required):
Connection Mode: Dial on Demand
Idle Timeout (In Minutes): 5

Internet IP Address
● Get Dynamically From ISP
○ Use Static IP Address: 0 . 0 . 0 . 0

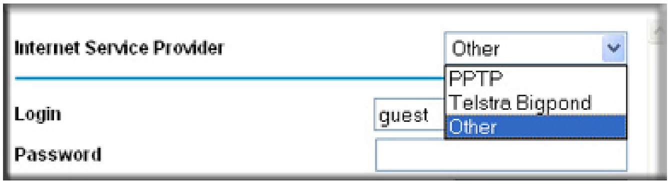
Domain Name Server (DNS) Address
○ Get Automatically From ISP
● Use These DNS Servers
Primary DNS: 206 . 13 . 28 . 12
Secondary DNS: 206 . 13 . 31 . 12

Figure 1-7

- **Does Your Internet Connection Require A Login?** If you usually must use a login program such as WinPOET to access the Internet, your Internet connection requires a login. After you select **Yes**, the Basic Settings screen displays.

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

- **Internet Service Provider**. This drop-down list contains a few ISPs that need special protocols for connection. Not all ISPs are listed here. The ones on this list have special requirements. The list includes:



Internet Service Provider: Other

Login: guest

Password:

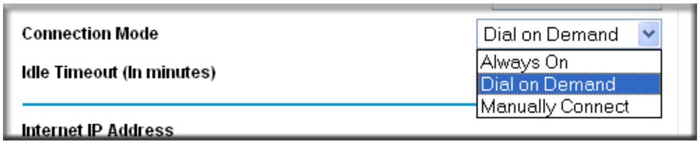
Figure 1-8

  - **PPTP** (Point to Point Tunneling Protocol), used primarily in Austrian DSL services
  - **Telstra Bigpond**, an Australian residential cable modem service

> **Note:** The Telstra Bigpond setting is only for older cable modem service accounts still requiring a Bigpond login utility. Telstra has discontinued this type of account. Those with Telstra DSL accounts and newer cable modem accounts should select **No** for Does Your Internet Connection Require a Login.

  - **Other**, which selects PPPoE (Point to Point Protocol over Ethernet), the protocol used by most DSL services worldwide.

- **Login and Password**. This is the user name and password provided by your ISP. This name and password are used to log in to the ISP server.
  - **Service Name**. If your connection is capable of connecting to multiple Internet services, this setting specifies which service to use.
  - **Connection Mode**. This drop-down list selects when the router will connect to and disconnect from the Internet. The list includes:



Connection Mode: Dial on Demand

Idle Timeout (In minutes)

Internet IP Address

Figure 1-9

    - **Always On**. The router logs in to the Internet immediately after booting and never disconnects.

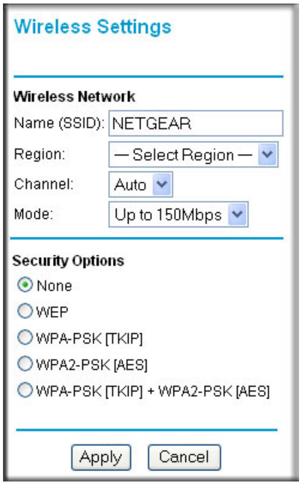
        - **Dial on Demand**. The router logs in only when outgoing traffic is present and logs out after the idle time-out.
        - **Manually Connect**. The router logs in or logs out only when the user clicks **Connect** or **Disconnect** in the Router Status screen.
    – **Idle Timeout**. Your Internet connection is logged out if there is no data transfer during the specified time interval.
- **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 or change a DNS address, restart the computers on your network so that these settings take effect.

Setting Up and Testing Basic Wireless Connectivity

Follow these instructions 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. Select **Wireless Settings** under Setup in the main menu of the WNR1000 v2h2 router.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: Auto

Mode: Up to 150Mbps

Security Options

● None

○ WEP

○ WPA-PSK [TKIP]

○ WPA2-PSK [AES]

○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Figure 1-10

2. As appropriate, select the region in which the wireless interface will operate.

> ➡ **Note:** In North America, you will not be able to change the region setting.

3. For the wireless network name (SSID), use the default name, or choose a suitable descriptive name. In the **Name (SSID)** field, you can 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 specify in the WNR1000 v2h2 router. If they do not match, you will not get a wireless connection to the WNR1000 v2h2 router.

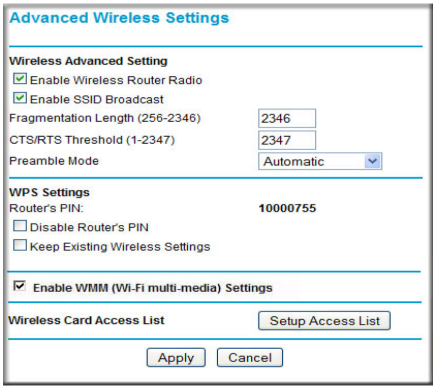
4. For the remaining settings, accept the defaults.
   - The default channel is **Auto**.

     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 router. For more information about the wireless channel frequencies, click the link to the online document "Wireless Networking Basics" in Appendix B.
   - The default mode of **Up to 150Mbps**. The options are:
     - Up to 54 Mbps – Legacy Mode – Maximum speed of up to 54 Mbps for b/g networks.
     - Up to 65 Mbps – Neighbor Friendly Mode – Will not interfere with neighboring wireless networks.
     - Up to 150 Mbps – Performance Mode – Maximum Wireless N speed up to 150 Mbps.
   - The default Security Options is **None**.

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

> ➡ **Note:** If you are configuring the router from a wireless computer and you change the router'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 router's new settings.

6. Select **Wireless Settings** under Advanced in the main menu of the WNR1000 v2h2 router.



Advanced Wireless Settings

Wireless Advanced Setting

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

Fragmentation Length (256-2346) 2346

CTS/RTS Threshold (1-2347) 2347

Preamble Mode Automatic

WPS Settings

Router's PIN: 10000755

□ Disable Router's PIN

□ Keep Existing Wireless Settings

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

Wireless Card Access List

Figure 1-11

7. Make sure that the **Enable Wireless Router Radio, Enable SSID Broadcast,** and **Enable WMM** check boxes are selected.

8. Click **Setup Access List**.

9. Make sure that the **Turn Access Control On** check box is *not* selected.

10. Configure and test your wireless computer for wireless connectivity.

Program the wireless adapter of your computer to have the same SSID and channel that you specified in the router, and disable encryption. Check that your computer has a wireless link and can obtain an IP address by DHCP from the router.

Once your computer has basic wireless connectivity to the router, you can configure the advanced wireless security functions of the computer and router (for more information about security and these settings, see Chapter 2, "Safeguarding Your Network ").

Chapter 2
Safeguarding Your Network

The N 150 Wireless Router WNR1000 v2h2 provides highly effective security features, which are covered in detail in this chapter.

This chapter includes the following sections:

- "Choosing Appropriate Wireless Security"
- "Recording Basic Wireless Settings Setup Information" on page 2-5
- "Changing Wireless Security Settings" on page 2-6
- "Viewing Advanced Wireless Settings" on page 2-11
- "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13
- "Restricting Wireless Access by MAC Address" on page 2-18
- "Changing the Administrator Password" on page 2-20
- "Backing Up Your Configuration" on page 2-21
- "Understanding Your Firewall" on page 2-22

Choosing Appropriate Wireless Security

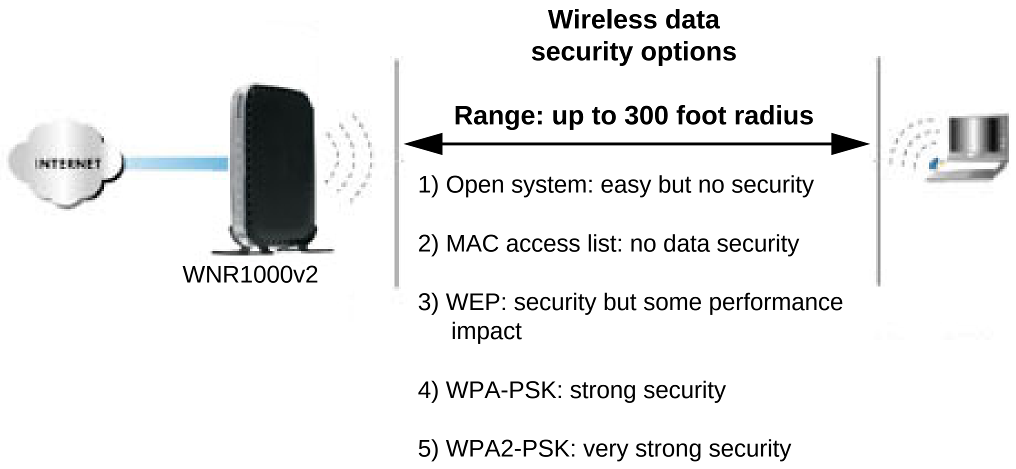
Unlike wired networks, wireless networks allow anyone with a compatible adapter to receive your wireless data transmissions well beyond your walls. Operating an unsecured wireless network creates an opportunity for outsiders to eavesdrop on your network traffic or to enter your network to access your computers and files. Indoors, computers can connect over wireless networks at ranges of up to 300 feet. Such distances can allow for others outside your immediate area to access your network. Use the security features of your wireless equipment that are appropriate to your needs.

The time it takes to establish a wireless connection can vary depending on both your security settings and router placement.

Stronger security methods can entail a cost in terms of throughput, latency, battery consumption, and equipment compatibility. In choosing an appropriate security level, you can also consider the effort compared to the reward for a hacker to break into your network. As a minimum, however, NETGEAR recommends using WEP with Shared Key authentication. Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public.

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, and can cause significant performance degradation with a slow computer.

Note: NETGEAR recommends that you change the administration password of your router. Default passwords are well known, and an intruder can use your administrator access to read or disable your security settings. For information about how to change the administrator password, see "Changing the Administrator Password" on page 2-20.



Wireless data security options

1) Open system: easy but no security

2) MAC access list: no data security

3) WEP: security but some performance impact

4) WPA-PSK: strong security

5) WPA2-PSK: very strong security

Note: Use these with other features that enhance security (Table 2-2 on page 2-4).

Figure 2-1

To configure the wireless network, you can:

- **Manually specify your SSID and your wireless security settings**. The WNR1000 v2h2 router provides two screens for configuring the wireless settings:
  - **Wireless Settings**. You access these under Setup in the main menu (see "Viewing Basic Wireless Settings" on page 2-6).
  - **Advanced Wireless Settings**. You access these under Advanced in the main menu (see "Viewing Advanced Wireless Settings" on page 2-11).

- **Use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security on both the router and the client device**. If the clients in your network are WPS capable, you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security on both the router and the client device (see "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13).

Basic security options are listed in order of increasing effectiveness in Table 2-1. Other features that affect security are listed in Table 2-2 on page 2-4. For more details on wireless security methods, click the link to the online document "Wireless Networking Basics" in Appendix B.

Table 2-1. Wireless Security Options

Security Type	Description
None.	No wireless security. Recommended only for troubleshooting wireless connectivity. Do not run an unsecured wireless network unless it is your intention to provide free Internet access for the public.
WEP. Wired Equivalent Privacy.	Wired Equivalent Privacy (WEP) data encryption provides moderate data security. WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools. For more information, see "Configuring WEP Wireless Security" on page 2-8.
WPA-PSK (TKIP). WPA-PSK standard encryption with TKIP encryption type. **WPA2-PSK (AES)**. Wi-Fi Protected Access version 2 with Pre-Shared Key; WPA2-PSK standard encryption with the AES encryption type. **WPA-PSK (TKIP) + WPA2-PSK (AES)**. Mixed mode.	Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provides extremely strong data security, very effectively blocking eavesdropping. Because WPA and WPA2 are relatively new standards, older wireless adapters and devices might not support them. For more information, see "Configuring WPA-PSK and WPA2-PSK Wireless Security" on page 2-10.

Table 2-2. Other Features That Enhance Security

Security Type	Description
Disable the wireless router radio.	If you disable the wireless router radio, wireless devices cannot communicate with the router at all. You might disable this when you are away or when other users of your network all use wired connections. For more information, see "Viewing Advanced Wireless Settings" on page 2-11.
Turn off the broadcast of the wireless network name SSID.	If you disable the broadcast of the SSID, only devices that know the correct SSID can connect. This nullifies the wireless network discovery feature of some products such as Windows XP, but your data is still fully exposed to an intruder using available wireless eavesdropping tools. For more information, see "Viewing Advanced Wireless Settings" on page 2-11.
Restrict access based on MAC address.	You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WNR1000v2 router. MAC address filtering adds an obstacle against unwanted access to your network by the general public, but the data broadcast over the wireless link is fully exposed. This data includes your trusted MAC addresses, which can be read and impersonated by a hacker. For more information, see "Restricting Wireless Access by MAC Address" on page 2-18.
Modify your firewall's rules.	By default, the firewall allows any outbound traffic and prohibits any inbound traffic except for responses to your outbound traffic. However, you can modify the firewall's rules. For more information, see "Understanding Your Firewall" on page 2-22.
Use the Push 'N' Connect feature (Wi-Fi Protected Setup).	Wi-Fi Protected Setup provides easy setup by means of a push button. Older wireless adapters and devices might not support this. Check whether devices are WPS enabled. For more information, see "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13.

Recording Basic Wireless Settings Setup Information

Before and after customizing your wireless settings, print this section, 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 can 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 provided.

- **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: **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 provided.

    - **Passphrase Method**. ______________________________ These characters *are* case-sensitive. Enter a word or group of printable characters and click Generate. Not all wireless devices support the passphrase method.
    - **Manual Method**. These values *are not* case-sensitive. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F). For 128-bit WEP, enter 26 hexadecimal digits.

      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 also set to WPA-PSK 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 specify the WNR1000 v2h2 router. Store this information in a safe place.

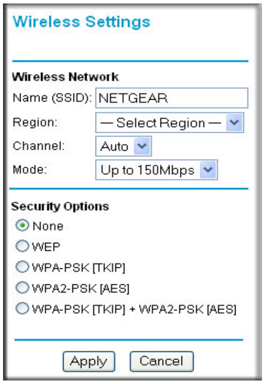
Changing Wireless Security Settings

This section describes the wireless settings that you can view and configure in the Wireless Settings screen, which you access under Setup in the main menu.

Viewing Basic Wireless Settings

To specify the wireless security settings of your router:

1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2.
2. Select **Wireless Settings** under Setup in the main menu. The Wireless Settings screen displays**.**



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: Auto

Mode: Up to 150Mbps

Security Options

● None

○ WEP

○ WPA-PSK [TKIP]

○ WPA2-PSK [AES]

○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Figure 2-2

The available settings in this screen are:

- **Name (SSID)**. The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. When more than one wireless network is active, different wireless network names provide a way to separate the traffic. For a wireless device to participate in a particular wireless network, it must be configured with the SSID for that network. The WNR1000 v2h2 default SSID is **NETGEAR**. You can disable this broadcast as described in "Viewing Advanced Wireless Settings" on page 2-11.
- **Region**. This field identifies the region where the WNR1000 v2h2 router can be used. It might 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 might 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 wireless network. The wireless router uses channel bonding technology to extend the bandwidth for data transmission. For more information about the wireless channel frequencies, see the online document that you can access from "Wireless Networking Basics" in Appendix B.
- **Mode**. The default mode is **Up to 150Mbps**.

> **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.

The Mode options are:

– Up to 54 Mbps - Legacy Mode with maximum speed of up to 54 Mbps for b/g networks.

– Up to 65 Mbps - Neighbor Friendly Mode - Will not interfere with neighboring wireless networks.

  - Up to 150 Mbps - Performance Mode - Maximum Nx speeds up to 150 Mbps. Using channel expansion to achieve the 150 Mbps data rate, the WNR1000 v2h2 will use the channel you selected as the primary channel and expand to the secondary channel (primary channel +4 or –4) to achieve a 40 MHz frame-by-frame bandwidth. The WNR1000 v2h2 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.

- **Security Options**. The selection of wireless security options can significantly affect your network performance. The time it takes to establish a wireless connection can vary depending on both your security settings and router 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, and can cause significant performance degradation with a slow computer. Instructions for configuring the security options can be found in "Choosing Appropriate Wireless Security" on page 2-1. A full explanation of wireless security standards is available in the online document that you can access from "Wireless Networking Basics" in Appendix B.

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

Configuring WEP Wireless Security

WEP Shared Key authentication and WEP data encryption can be defeated by a determined eavesdropper using publicly available tools.

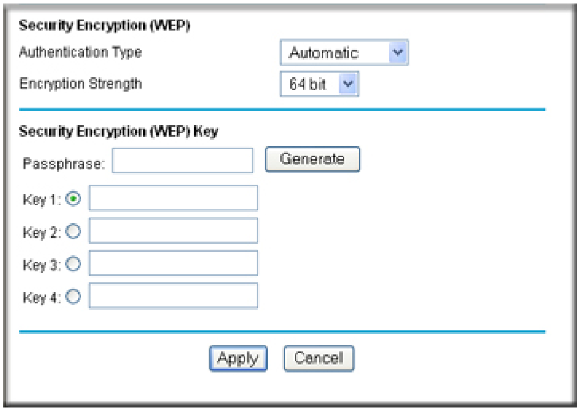
WEP offers the following options:

- **Automatic**. With the Automatic option, the router will try both Open System and Shared Key authentication. Normally this setting is suitable. If it fails, select **Open System** or **Shared Key**. You can also refer to your wireless adapter's documentation to see what method to use.
- **Open System**. With Open System authentication and 64 or 128 bit WEP data encryption, the WNR1000 v2h2 router *does* perform data encryption but *does not* perform any authentication. Anyone can join the network. This setting provides very little practical wireless security.
- **Shared Key**. With Shared Key authentication, a wireless device must know the WEP key to join the network. Select 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** field. Manually entered keys *are not* case-sensitive, but passphrase characters *are* case-sensitive.

To configure WEP data encryption:

> **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. Not all wireless adapter configuration utilities support passphrase key generation.

1. Select **Wireless Settings** under Setup in the main menu.
2. In the Security Options section, select **WEP**. The WEP options display.



Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: 64 bit

Security Encryption (WEP) Key

Passphrase:

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Figure 2-3

3. Select the authentication type and encryption strength.
4. 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**. In the **Passphrase** field, enter a word or group of printable characters, and click **Generate**. The passphrase is case-sensitive. For example, NETGEAR is not the same as nETgear. The four key fields are automatically populated with key values.
   - **Manual**. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F). These entries are not case-sensitive. For example, AA is the same as aa.
     Select which of the four keys to activate.
5. Click **Apply** to save your settings.

Configuring WPA-PSK and WPA2-PSK Wireless Security

Wi-Fi Protected Access with Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provides extremely strong data security, very effectively blocking eavesdropping. Because WPA and WPA2 are relatively new standards, older wireless adapters and devices might not support them. Check whether newer drivers are available from the manufacturer. Also, you might be able to use the Push 'N' Connect feature to configure this type of security if it is supported by your wireless clients. See "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13.

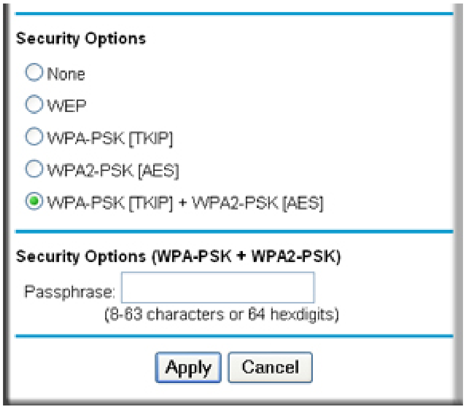
WPA–Pre-Shared Key *does* perform authentication. WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption, and WPA2-PSK uses AES (Advanced Encryption Standard) data encryption. Both methods dynamically change the encryption keys making them nearly impossible to circumvent.

Mixed mode allows clients using either WPA-PSK (TKIP) or WPA2-PSK (AES). This provides the most reliable security, and is easiest to implement, but it might not be compatible with older adapters.

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, WPA2-PSK, or WPA-PSK+WPA2-PSK:

1. Select **Wireless Settings** under Setup in the main menu. The Wireless Settings screen displays.
2. 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.
3. In the **Passphrase** field, enter a word or group of 8–63 printable characters. The passphrase is case-sensitive.



Security Options

○ None
○ WEP
○ WPA-PSK [TKIP]
○ WPA2-PSK [AES]
● WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Options (WPA-PSK + WPA2-PSK)

Passphrase:
(8-63 characters or 64 hexdigits)

Figure 2-4

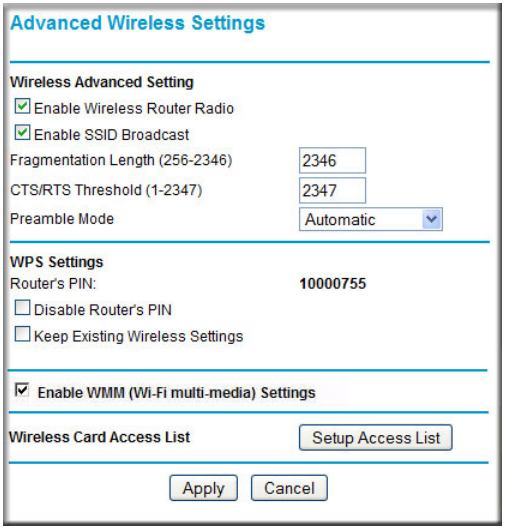
4. Click **Apply** to save your settings.

Viewing Advanced Wireless Settings

This section describes the wireless settings that you can view and specify in the Advanced Wireless Settings screen, which you access under Advanced in the main menu.

To configure the advanced wireless security settings of your router:

1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2.
2. Select **Wireless Settings** under Advanced in the main menu. The advanced Wireless Settings screen displays



Advanced Wireless Settings

Wireless Advanced Setting

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

Fragmentation Length (256-2346) 2346

CTS/RTS Threshold (1-2347) 2347

Preamble Mode Automatic

WPS Settings

Router's PIN: 10000755

☐ Disable Router's PIN

☐ Keep Existing Wireless Settings

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

Wireless Card Access List

Figure 2-5

The available settings in this screen are:

- **Enable Wireless Router Radio**. If you disable the wireless router radio, wireless devices cannot connect to the WNR1000 v2h2 router. If you will not be using your wireless network for a period of time, you can clear this check box and disable all wireless connectivity.
- **Enable SSID Broadcast**. Clear this check box to disable broadcast of the SSID, so that only devices that know the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP.
- **Enable WMM**. Clear this check box to disable WMM. WMM (Wireless Multimedia), a subset of the 802.11e standard, allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, will have a higher priority than normal traffic. For WMM to function correctly, Wireless clients must also support WMM.
- **Fragmentation Threshold**, **CTS/RTS Threshold**, and **Preamble Mode**. The Fragmentation Threshold, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.
- **WPS Settings**. For information about these settings, see the section, “Using Push 'N' Connect (Wi-Fi Protected Setup)” on page 2-13.
- **Wireless Card Access List**. For information about this list, see “Restricting Wireless Access by MAC Address” on page 2-18.

Using Push 'N' Connect (Wi-Fi Protected Setup)

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

Note: NETGEAR's Push 'N' Connect feature is based on the Wi-Fi Protected Setup (WPS) standard (for more information, see *http://www.wi-fi.org*). All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.

When you add wireless clients, whether or not they are WPS enabled, the added devices must share the same network name (SSID) and security passphrase. For more information, see "Connecting Additional Wireless Client Devices after WPS Setup" on page 2-17.

Note: If you choose to use WPS, the only security methods supported are WPA-PSK and WPA2-PSK. WEP security is not supported by WPS.

The WNR1000v2 router provides two methods for connecting to a wireless client that supports WPS, described in the following sections:

- "Push Button Configuration"
- "Security PIN Entry" on page 2-15

Push Button Configuration

There are two methods to enable a wireless client to join a network using a push button on the router: using the physical push button or using the software button in the Add WPS Client screen.

Using the Physical Push Button

1. Press the button on the rear of the WNR1000 v2h2 router for over 5 seconds. For information about the WPS light, see the *NETGEAR Wireless Router Setup Manual*.

   The green light begins to blink in a regular pattern. While the light is blinking, you have 2 minutes to enable WPS on the client that you are trying to connect to the router.

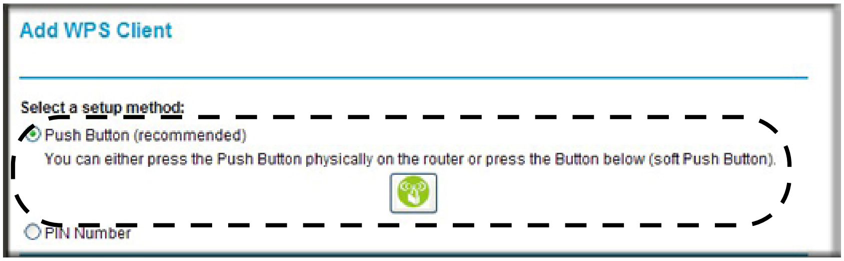
2. On the wireless client, follow its specific networking instructions to enable WPS, to allow it to connect to the router.

   The WNR1000 v2h2 router's gre light ceases blinking and remains on when one of these conditions occurs:

   - The router and the client establish a wireless connection.
   - The 2-minute window period expires for establishing a WPS connection. If the connection is not established, no WPS security settings will be specified in the WNR1000 v2h2 router.

Using the Software Button in the Add WPS Client Screen

1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2.
2. Select **Add WPS Client** in the main menu, and click **Next.**
3. Select the **Push Button** setup method.



Add WPS Client

Select a setup method:

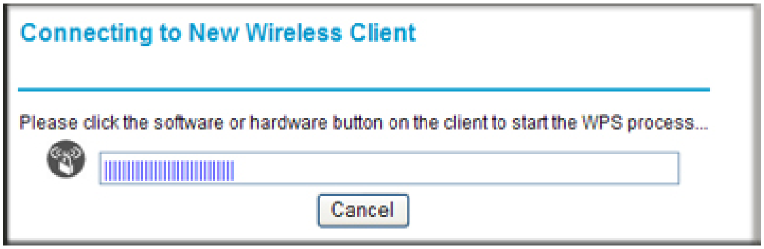
● Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button).

○ PIN Number

Figure 2-6

4. Click the button in the Add WPS Client screen. The Connecting to New Wireless Client screen displays.



Connecting to New Wireless Client

Please click the software or hardware button on the client to start the WPS process...

Cancel

Figure 2-7

The green light on the WNR1000 v2h2 router begins to blink in a regular pattern. While the button light is blinking, you have 2 minutes to enable WPS on the device you are trying to connect to the router.

5. In the wireless client, follow its specific networking instructions to enable WPS, to allow it to connect to the router.

   The WNR1000 v2h2 router's gre light ceases blinking and remains on when one of these conditions occurs:

   - The router and the client establish a wireless connection.
   - The 2-minute window period expires for establishing a WPS connection. If the connection is not established, no WPS security settings will be specified in the WNR1000 v2h2 router.

Security PIN Entry

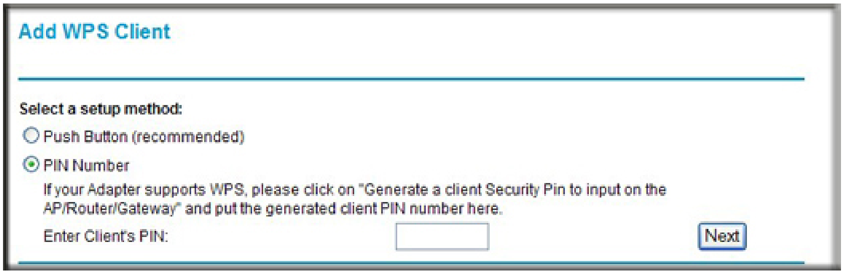
There are two ways to enable a wireless client to join a network using a PIN: using the router's security PIN or using the wireless client's security PIN.

Using the Router's Security PIN

1. Obtain your router's security PIN from the rear panel of the router or from the Advanced Wireless Settings screen.
2. On the wireless client, follow its specific networking instructions to enter the router's security PIN and to establish a wireless connection with the router.

Using the Wireless Client's Security PIN

1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2.
2. Select **Add WPS Client** in the main menu, and click **Next**.
3. Select the **PIN Number** setup method.



Add WPS Client

Select a setup method:

○ Push Button (recommended)

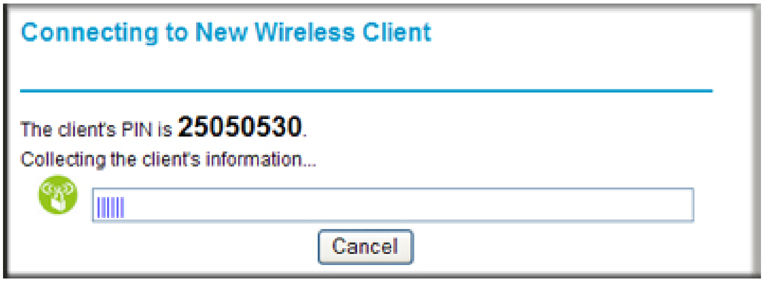
● PIN Number

If your Adapter supports WPS, please click on "Generate a client Security Pin to input on the AP/Router/Gateway" and put the generated client PIN number here.

Enter Client's PIN:

Figure 2-8

4. On the wireless client, obtain its security PIN, or follow its specific networking instructions to generate a client security PIN.
5. In the Add WPS Client screen of the WNR1000 v2h2 router, enter the client security PIN in the **Enter Client's PIN** field.
6. Click **Next**. The following screen displays, and the Smart Wizard initiates the wireless connection:



Connecting to New Wireless Client

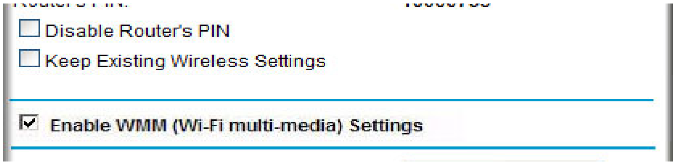
The client's PIN is **25050530**.

Collecting the client's information...

Figure 2-9

Configuring the WPS Settings

1. Log in to the router as described in "Logging In To Your Wireless Router" on page 1-2.
2. Select **Wireless Settings** under Advanced in the main menu.



□ Disable Router's PIN

□ Keep Existing Wireless Settings

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

Figure 2-10

These options are available under WPS Settings:

- **Router's PIN**. The PIN is displayed so that you can use it to configure the router through WPS (Wi-Fi Protected Setup). It is also displayed on the router's label.
- **Disable Router's PIN**. If the router's PIN is disabled, you cannot configure the router's wireless settings with WPS. However, if your settings are already configured, you can still add WPS-enabled wireless clients. The router might disable the PIN if it detects suspicious attempts to break into your wireless settings; this can happen if the check box is selected. You can enable the PIN by clearing the check box and clicking **Apply**.
- **Keep Existing Wireless Settings**. This check box is automatically selected after WPS is enabled to prevent unwanted settings changes, and is also selected if you have already specified wireless security settings or your SSID without using WPS. When this check box is *not* selected, adding a new wireless client using the push button or the Add WPS Client screen (see "Push Button Configuration" on page 2-13) changes the router's SSID and security passphrase. You might need to clear it if you are using certain registrars, such as for a Windows Vista PC, to configure the router through WPS.

Connecting Additional Wireless Client Devices after WPS Setup

You can add WPS-enabled and non-WPS-enabled client devices.

Adding Additional WPS-Enabled Clients

To add an additional wireless client device that is WPS enabled:

> **Note:** Your wireless settings do not change when you add an additional WPS-enabled client unless you have cleared the **Keep Existing Wireless Settings** check box (in the Wireless Settings screen). If you do clear the check box, a new SSID and a passphrase are generated, and all existing connected wireless clients are disassociated and disconnected from the router.

1. Follow the procedures in "Push Button Configuration" on page 2-13 or "Security PIN Entry" on page 2-15.
2. For information about how to view a list of all devices connected to your router (including wireless and Ethernet-connected), see "Viewing a List of Attached Devices" on page 6-7.

Adding Additional Non-WPS-Enabled Clients

If you are connecting a combination of WPS-enabled clients and clients that are not WPS enabled, you cannot use the WPS setup procedures to add clients that are not WPS enabled.

To connect both non-WPS-enabled and WPS-enabled clients to the WNR1000 v2h2 router:

1. Configure the settings of the WNR1000 v2h2 router (shown in the Wireless Settings screen) for WPA-PSK or WPA2-PSK security, and record that information. See "Configuring WPA-PSK and WPA2-PSK Wireless Security" on page 2-10.

   When you change security settings, all existing connected wireless clients that do not share those settings are disassociated and disconnected from the router.
2. For the non-WPS-enabled devices that you wish to connect, open the networking utility, and follow the utility's instructions to enter security settings.
3. For the WPS-enabled devices that you wish to connect, follow the procedures in "Using Push 'N' Connect (Wi-Fi Protected Setup)" on page 2-13.

   The WNR1000 v2h2 router automatically preserves the settings you configured in step 1 so all clients share the same security settings (for more information, see "Configuring the WPS Settings" on page 2-16).
4. For information about how to view a list of all devices connected to your router (including wireless and Ethernet connected), see "Viewing a List of Attached Devices" on page 6-7.

Restricting Wireless Access by MAC Address

When a Wireless Card Access List is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computers list.

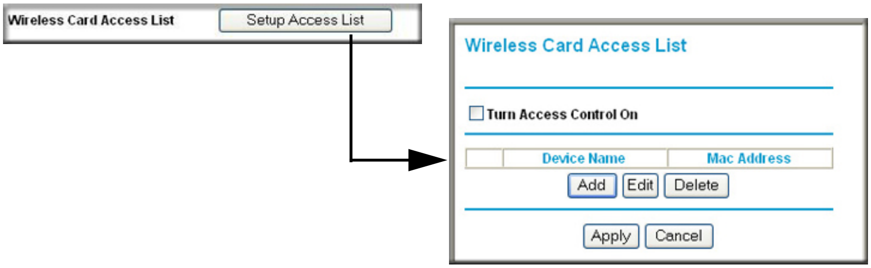
The Wireless Card Access List displays a list of wireless computers that you allow to connect to the router based on their MAC addresses. These wireless computers must also have the correct SSID and wireless security settings to access the wireless router.

The MAC address is a network device's unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). It can usually be found on the bottom of the wireless card or network interface device. If you do not have access to the physical label, you can display the MAC address using the network configuration utilities of the computer. In WindowsXP, for example, typing the **`ipconfig/all`** command in an MSDOS command prompt window displays the MAC address as Physical Address. You might also find the MAC addresses in the router's Attached Devices screen.

To restrict access based on MAC addresses:

1. Select **Wireless Settings** under Advanced in the main menu.

2. In the Advanced Wireless Settings screen, click **Setup Access List** to display the Wireless Card Access List.



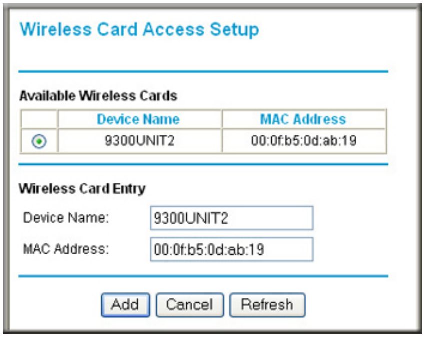
Wireless Card Access List

□ Turn Access Control On

	Device Name	Mac Address

Figure 2-11

3. Click **Add** to add a wireless device to the wireless access control list. The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.



Wireless Card Access Setup

Available Wireless Cards

	Device Name	MAC Address
◉	9300UNIT2	00:0f:b5:0d:ab:19

Wireless Card Entry

Device Name: 9300UNIT2

MAC Address: 00:0f:b5:0d:ab:19

Figure 2-12

4. If the computer you want appears in the Available Wireless Cards list, you can select the radio button of that computer to capture its MAC address; otherwise, you can manually enter a name and the MAC address of the authorized computer. You can usually find the MAC address on the bottom of the wireless device.

Tip: You can copy and paste the MAC addresses from the router’s Attached Devices screen into the MAC Address field of this screen. To do this, configure each wireless computer to obtain a wireless link to the router. The computer should then appear in the Attached Devices screen.

5. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.
6. Repeat step 3 through step 5 for each additional device you want to add to the list.
7. Select the **Turn Access Control On** check box.

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

8. Click **Apply** to save your Wireless Card Access List settings.

   Now, only devices on this list can wirelessly connect to the WNR1000 v2h2 router.

⚠	**Warning:** MAC address filtering adds an obstacle against unwanted access to your network by the general public. However, because your trusted MAC addresses appear in your wireless transmissions, an intruder can read them and impersonate them. Do not rely on MAC address filtering alone to secure your network.

Changing the Administrator Password

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

💡	**Tip:** Before changing the router password, back up your configuration settings with the default password of **password**. If you save the settings with a new password, and then you later forget the new password, you will have to reset the router back to the factory defaults, and log in using the default password of **password**. This means you will have to re-enter all the router configuration settings. For information about how to back up your settings, see "Backing Up and Restoring the Configuration" on page 6-8.

To change the administrator password:

1. On the main menu, under Maintenance, select **Set Password** to display the Set Password screen.

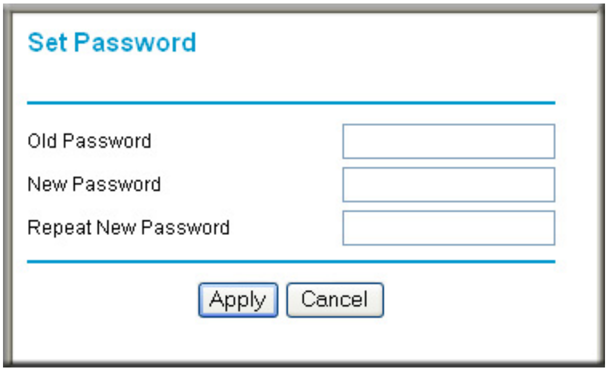


Figure 2-13

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

Backing Up Your Configuration

The configuration settings of the WNR1000 v2h2 router are stored within the router in a configuration file. You can back up (save) this file and retrieve it later. NETGEAR recommends that you save your configuration file after you complete the configuration. If the router fails or becomes corrupted, or an administrator password is lost, you can easily re-create your configuration by restoring the configuration file.

For instructions on saving and restoring your configuration file, see “Managing the Configuration File” on page 6-7.

Tip: Before saving your configuration file, change the administrator password to the default, **password**. Then change it again after you have saved the configuration file. If you save the file with a new password, and then you later forget the new password, you will have to reset the router back to the factory defaults and log in using the default password of **password**. This means you will have to re-enter all the router configuration settings.

Understanding Your Firewall

Your N 150 Wireless Router WNR1000 v2h2 contains a true firewall to protect your network from attacks and intrusions. A firewall is a device that protects one network from another while allowing communication between the two. Using a process called Stateful Packet Inspection, the firewall analyzes all inbound and outbound traffic to determine whether or not it will be allowed to pass through.

By default, the firewall allows any outbound traffic and prohibits any inbound traffic except for responses to your outbound traffic. However, you can modify the firewall's rules to achieve the following behavior:

- **Blocking sites**. Block access from your network to certain Web locations based on Web addresses and Web address keywords. This feature is described in "Blocking Access to Internet Sites" on page 3-1.
- **Blocking services**. Block the use of certain Internet services by specific computers on your network. This feature is described in "Blocking Access to Internet Services" on page 3-3.
- **Scheduled blocking**. Block sites and services according to a daily schedule. This feature is described in "Scheduling Blocking" on page 3-5.
- **Allow inbound access to your server**. To allow inbound access to resources on your local network (for example, a Web server or remote desktop program), you can open the needed services by configuring port forwarding as described in "Allowing Inbound Connections to Your Network" on page 5-1.
- **Allow certain games and applications to function correctly**. Some games and applications need to allow additional inbound traffic in order to function. Port triggering can dynamically allow additional service connections, as described in "Configuring Port Triggering" on page 5-9. Another feature to solve application conflicts with the firewall is Universal Plug and Play (UPnP), described in "Using Universal Plug and Play" on page 5-12.

Chapter 3
Restricting Access From Your Network

This chapter describes how to use the content filtering and reporting features of the N 150 Wireless Router WNR1000 v2h2 to protect your network.

This chapter includes the following sections:

- "Content Filtering Overview"
- "Blocking Access to Internet Sites"
- "Blocking Access to Internet Services" on page 3-3
- "Scheduling Blocking" on page 3-5
- "Viewing Logs of Web Access or Attempted Web Access" on page 3-6
- "Configuring E-mail Alert and Web Access Log Notifications" on page 3-7
- "Setting the Time Zone" on page 3-8

Content Filtering Overview

The N 150 Wireless Router WNR1000 v2h2 provides you with Web content filtering options, plus browser activity reporting and instant alerts through 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 rooms or games.

Blocking Access to Internet Sites

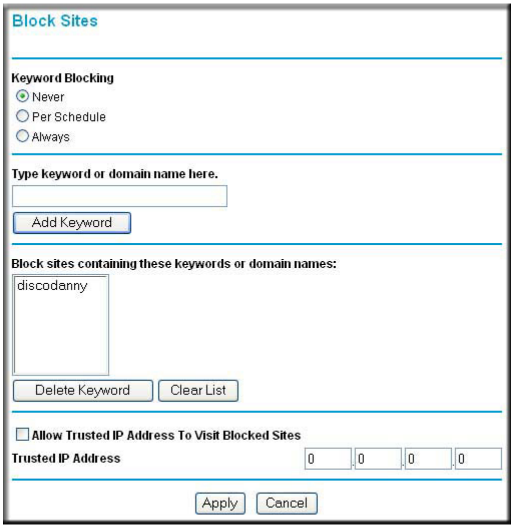
The WNR1000 v2h2 router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list.

Keyword application examples:

- If the keyword **XXX** is specified, the URL www.zzzyyqq.com/xxx.html is blocked.
- If the keyword **.com** is specified, only websites with other domain suffixes (such as .edu, .org, or .gov) can be viewed.

To block access to Internet sites:

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



Block Sites

Keyword Blocking

● Never
○ Per Schedule
○ Always

Type keyword or domain name here.

Block sites containing these keywords or domain names:

discodanny

□ Allow Trusted IP Address To Visit Blocked Sites

Trusted IP Address 0 . 0 . 0 . 0

Figure 3-1

2. Enable keyword blocking by selecting either **Per Schedule** or **Always**.

   To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see "Scheduling Blocking" on page 3-5.

   Block all access to Internet browsing during a scheduled period by entering a dot (**.**) as the keyword, and then set a schedule in the Schedule screen.

3. Add a keyword or domain by entering it in the keyword field and clicking **Add Keyword**. The keyword or domain name then appears the **Block sites containing these keywords or domain names** list.

   Delete a keyword or domain name by selecting it from the list and clicking **Delete Keyword**.

4. You can specify one trusted user, which is a computer that is exempt from blocking and logging. Specify a trusted user by entering that computer's IP address in the **Trusted IP Address** fields.

   Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address.

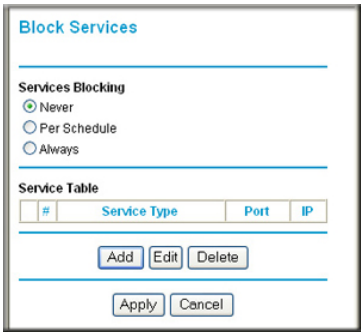
5. Click **Apply** to save all your settings in the Block Sites screen.

Blocking Access to Internet Services

The WNR1000 v2h2 router allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. 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 block access to Internet services:

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



Block Services

Services Blocking

● Never

○ Per Schedule

○ Always

Service Table

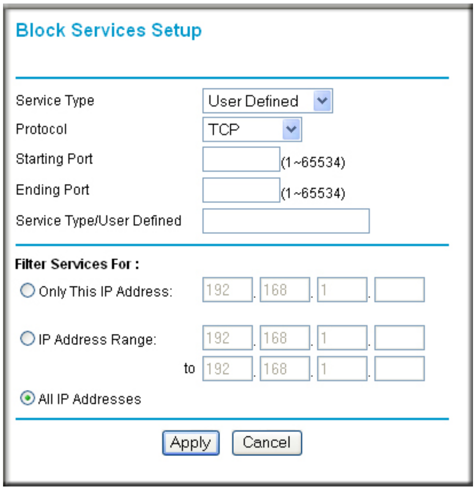
	#	Service Type	Port	IP

Figure 3-2

2. Enable service blocking by selecting either **Per Schedule** or **Always**, and then click **Apply**.

   To block by schedule, be sure to specify a time period in the Schedule screen. For information about scheduling, see "Scheduling Blocking" on page 3-5.

3. Specify a service for blocking by clicking **Add**. The Block Services Setup screen displays.



Block Services Setup

Service Type: User Defined
Protocol: TCP
Starting Port: (1~65534)
Ending Port: (1~65534)
Service Type/User Defined:

Filter Services For :
○ Only This IP Address: 192 . 168 . 1 .
○ IP Address Range: 192 . 168 . 1 .
to 192 . 168 . 1 .
● All IP Addresses

Figure 3-3

4. 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**. To define a service, first you must determine which port number or range of numbers is used by the application. The service port 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. You can often determine port number information by contacting the publisher of the application, by asking user groups or newsgroups, or by searching.

   – Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both fields.

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

5. Select the radio button for the IP address configuration you want to block, and then enter the IP addresses in the appropriate fields.

6. Click **Add** to enable your Block Services Setup selections.

Blocking Services by IP Address Range

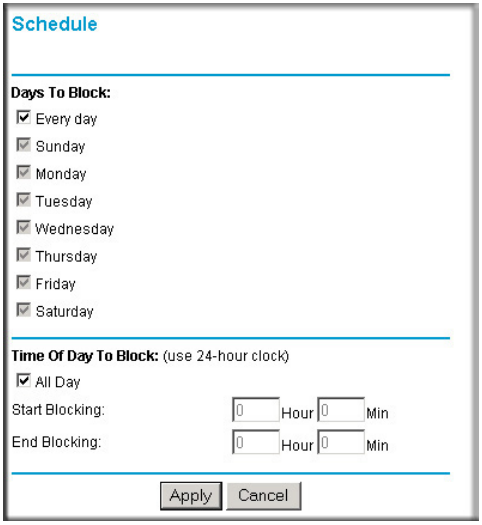
In the Filter Services For area, you can block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Scheduling Blocking

TheWNR1000 v2h2 router allows you to specify when blocking is enforced.

To schedule blocking:

1. Select **Schedule** under Content Filtering in the main menu. The Schedule screen displays.



Schedule

Days To Block:

☑ Every day
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Time Of Day To Block: (use 24-hour clock)

☑ All Day

Start Blocking: 0 Hour 0 Min

End Blocking: 0 Hour 0 Min

Figure 3-4

2. Configure the schedule for blocking keywords and services.
   a. **Days to Block**. Select days on which you want to apply blocking by selecting the appropriate check boxes. Select **Every Day** to select the check boxes for all days. Click **Apply**.
   b. **Time of Day to Block**. Select a start and end time in 24-hour format. Select **All Day** for 24-hour blocking. Click **Apply**.

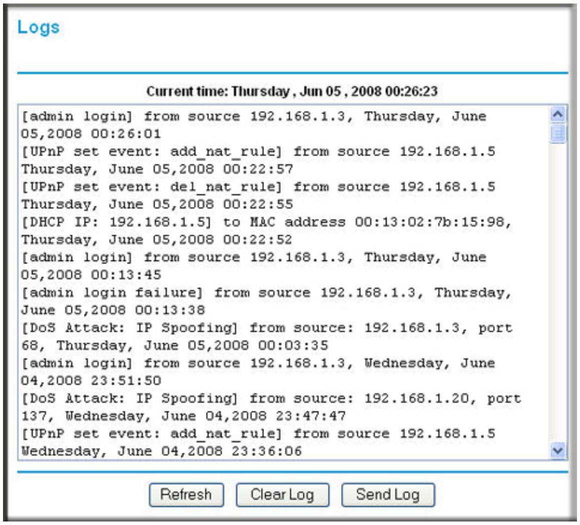
   Be sure to select your time zone in the E-mail screen as described in "Setting the Time Zone" on page 3-8.

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

Viewing Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 128 entries are stored in the log. Log entries appear only when keyword blocking is enabled and no log entries are made for the trusted user.

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



Current time: Thursday , Jun 05 , 2008 00:26:23

```
[admin login] from source 192.168.1.3, Thursday, June
05,2008 00:26:01
[UPnP set event: add_nat_rule] from source 192.168.1.5
Thursday, June 05,2008 00:22:57
[UPnP set event: del_nat_rule] from source 192.168.1.5
Thursday, June 05,2008 00:22:55
[DHCP IP: 192.168.1.5] to MAC address 00:13:02:7b:15:98,
Thursday, June 05,2008 00:22:52
[admin login] from source 192.168.1.3, Thursday, June
05,2008 00:13:45
[admin login failure] from source 192.168.1.3, Thursday,
June 05,2008 00:13:38
[DoS Attack: IP Spoofing] from source: 192.168.1.3, port
68, Thursday, June 05,2008 00:03:35
[admin login] from source 192.168.1.3, Wednesday, June
04,2008 23:51:50
[DoS Attack: IP Spoofing] from source: 192.168.1.20, port
137, Wednesday, June 04,2008 23:47:47
[UPnP set event: add_nat_rule] from source 192.168.1.5
Wednesday, June 04,2008 23:36:06
```

Figure 3-5

Table 3-1 describes the log entries.

Table 3-1. 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 website or newsgroup visited or to which access was attempted.
Action	Whether the access was blocked or allowed.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

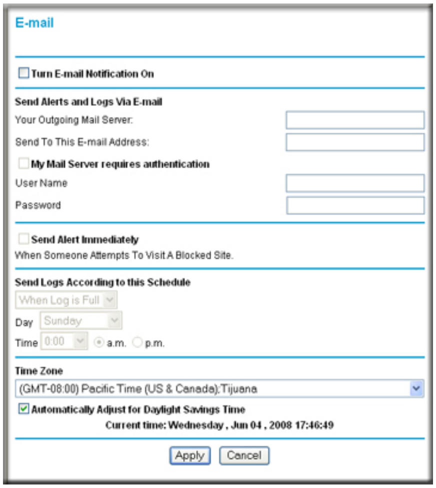
To e-mail the log immediately, click the **Send Log** button.

Configuring E-mail Alert and Web Access Log Notifications

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

To configure e-mail alert and web access log notifications:

1. Select **E-mail** under Content Filtering in the main menu. The E-mail screen displays.



E-mail

□ **Turn E-mail Notification On**

Send Alerts and Logs Via E-mail

Your Outgoing Mail Server:

Send To This E-mail Address:

□ **My Mail Server requires authentication**

User Name

Password

□ **Send Alert Immediately**

When Someone Attempts To Visit A Blocked Site.

Send Logs According to this Schedule

When Log is Full

Day Sunday

Time 0:00 ● a.m. ○ p.m.

Time Zone

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

☑ **Automatically Adjust for Daylight Savings Time**

Current time: Wednesday , Jun 04 , 2008 17:46:49

Figure 3-6

2. To receive e-mail logs and alerts from the router, select the **Turn E-mail Notification On** check box.

   a. Enter the name of your ISP’s outgoing (SMTP) mail server (such as **mail.myISP.com**) in the **Your Outgoing Mail Server** field. You might be able to find this information in the configuration screen of your e-mail program. If you leave this field blank, log and alert messages will not be sent by e-mail.

   b. Enter the e-mail address to which logs and alerts are sent in the **Send To This E-mail Address** field. This e-mail address will also be used as the From address. If you leave this field blank, log and alert messages will not be sent by e-mail.

3. If your e-mail server requires authentication, select the **My Mail Server requires authentication** check box.

   a. Enter your user name for the e-mail server in the **User Name** field.

   b. Enter your password for the e-mail server in the **Password** field.

4. You can specify that logs are automatically sent by e-mail with these options:

   - **Send alert immediately**. Select this check box for immediate notification of attempted access to a blocked site or service.
   - **Send Logs According to this Schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
     - **Day**. Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
     - **Time**. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

   If you select the Weekly, Daily, or Hourly option 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 might fill up. In this case, the router overwrites the log and discards its contents.

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

So that the log entries are correctly time-stamped and sent at the correct time, be sure to set the time as described in the next section.

Setting the Time Zone

The WNR1000 v2h2 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. Localize the time zone so that your log entries and other router functions include the correct time stamp.

To verify and set the time zone (see Figure 3-6 on page 3-7):

- **Time Zone**. To select your local time zone, use the drop-down list. This setting is used for the blocking schedule and for time-stamping log entries.
- **Automatically Adjust for Daylight Savings Time**. If your region supports daylight savings time, select this check box . The router will automatically adjust the time at the start and end of the daylight savings time period.

Chapter 4
Customizing Your Network Settings

This chapter describes how to configure advanced networking features of the N 150 Wireless Router WNR1000 v2h2 , including LAN, WAN, and routing settings.

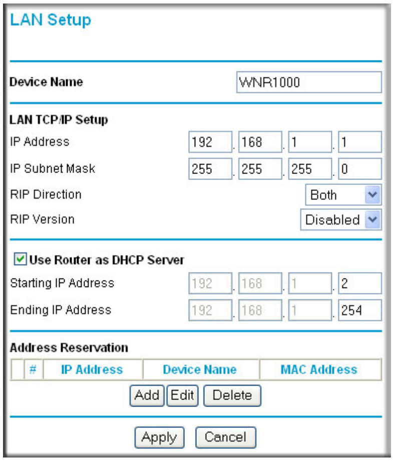
It contains the following sections:

- "Using the LAN IP Setup Options"
- "Using a Dynamic DNS Service" on page 4-5
- "Configuring the WAN Setup Options" on page 4-6
- "Configuring Static Routes" on page 4-8

Using the LAN IP Setup Options

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

To configure LAN IP settings, select **LAN Setup** under Advanced in the main menu. The LAN Setup screen displays.



LAN Setup

Device Name: WNR1000

LAN TCP/IP Setup

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: Both

RIP Version: Disabled

☑ Use Router as DHCP Server

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 254

Address Reservation

	#	IP Address	Device Name	MAC Address

Figure 4-1

Configuring a Device Name

The device name is a user-friendly name for the router. This name is shown in the Network on Windows Vista and the Network Explorer on all Windows systems. The **Device Name** field cannot be blank. The default name is WNR1000 v2h2.

Configuring LAN TCP/IP Setup Parameters

These are advanced settings that you might configure if you are a network administrator and your network contains multiple routers. The router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server (see "Using the Router as a DHCP Server" on page 4-3).

> **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.

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 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 screen.

The LAN IP settings are:

- **IP Address**. The LAN IP address of the router.
- **IP Subnet Mask**. 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 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 **In Only**, the router incorporates the RIP information that it receives.
  - When set to **Both** or **Out Only**, the router broadcasts its routing table periodically.
- **RIP Version**. This controls the format and the broadcasting method of the RIP packets sent by the router. (It recognizes both formats when receiving.) The default setting is **Disabled**.

- **RIP-1** is universally supported. RIP-1 is usually adequate unless you have an unusual network setup.
- **RIP-2B** carries more information than RIP-1 and uses subnet broadcasting.
- **RIP-2M** carries more information than RIP-1 and uses multicasting.

Using the Router as a DHCP Server

By default, the router functions as a DHCP 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 screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

Note: For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. Click the link to the online document "TCP/IP Networking Basics" in Appendix B for an explanation of DHCP and information about how to assign IP addresses for your network.

To specify a pool of IP addresses to be assigned, set 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 might wish to save part of the range for devices with fixed addresses.

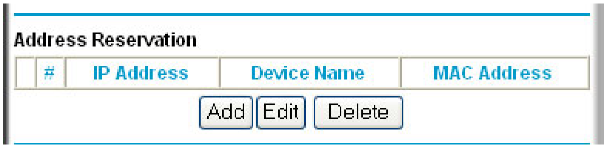
The router delivers the following parameters to any LAN device that requests DHCP:

- 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 screen; otherwise, the router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Basic Settings screen)

To use another device on your network as the DHCP server, or to manually specify the network settings of all of your computers, clear the **Use Router as DHCP Server** check box. Otherwise, leave it selected. If this service is not selected and no other DHCP server is available on your network, you need to set your computers' IP addresses manually or they will not be able to access the router.

Using Address Reservation

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



Address Reservation

	#	IP Address	Device Name	MAC Address

Figure 4-2

To reserve an IP address:

1. Click **Add**.
2. In the **IP Address** field, enter 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. Enter the MAC address of the computer or server.

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

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

> **Note:** The reserved address 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**.

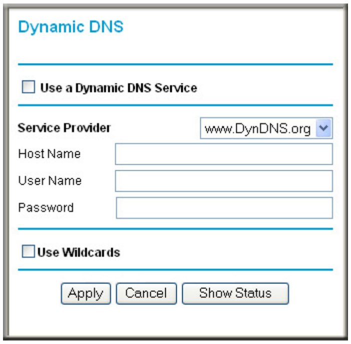
Using a Dynamic DNS Service

If your Internet Service Provider (ISP) gave you 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 allows you to register your domain to their IP address, and forwards 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.

Your router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. You must first visit their website at *www.dyndns.org* and obtain an account and host name, which you specify in the router. Then, whenever your ISP-assigned IP address changes, your router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host name is hostname, for example, you can reach your router at hostname.dyndns.org.

Select **Dynamic DNS** under Advanced in the main menu. The Dynamic DNS screen displays.



Dynamic DNS

□ Use a Dynamic DNS Service

Service Provider: www.DynDNS.org

Host Name

User Name

Password

□ Use Wildcards

Figure 4-3

To configure for a Dynamic DNS service:

1. Register for an account with one of the Dynamic DNS service providers whose names appear in the **Service Provider** list. For example, for DynDNS.org, select **www.dynDNS.org**.

2. Select the **Use a Dynamic DNS Service** check box.

3. Select the name of your Dynamic DNS service provider.

4. Enter the host name (or domain name) that your Dynamic DNS service provider gave you.

5. Enter the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.

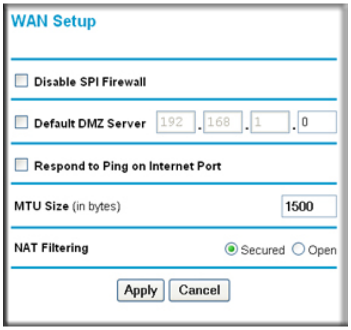
6. Enter the password (or key) for your Dynamic DNS account.

7. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature.
   For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.

8. Click **Apply** to save your configuration.

Configuring the WAN Setup Options

The WAN Setup options let you configure a DMZ (demilitarized zone) server, change the Maximum Transmit Unit (MTU) size, and enable the wireless router to respond to a ping on the WAN (Internet) port. Select **WAN Setup** under Advanced in the main menu. The WAN Setup screen displays.



WAN Setup

□ Disable SPI Firewall

□ Default DMZ Server 192 . 168 . 1 . 0

□ Respond to Ping on Internet Port

MTU Size (in bytes) 1500

NAT Filtering ● Secured ○ Open

Apply Cancel

Figure 4-4

Disabling the SPI Firewall

The Stateful Packet Inspection (SPI) firewall protects your network and computers against attacks and intrusions. A stateful packet firewall carefully inspects incoming traffic packets, looking for known exploits such as malformed, oversized, or out-of-sequence packets. The firewall should be disabled only in special circumstances, such as when you are troubleshooting application issues.

Setting Up a Default DMZ Server

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

> ⚠ **Warning:** 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 computer can be used to attack other computers on your network.

Incoming traffic from the Internet is usually 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 screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

The WAN Setup screen lets you configure a default DMZ server.

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

1. Select the **Default DMZ Server** check box.
2. In the **Default DMZ Server** fields, enter the IP address for that computer or server.
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, select the **Respond to Ping on Internet Port** check box. This should be used only as a diagnostic tool, since it allows your router to be discovered by Internet scanners. Do not select this check box unless you have a specific reason to do so, such as when troubleshooting your connection.

Setting the MTU Size

The normal MTU value for most Ethernet networks is 1500 bytes, 1492 bytes for PPPoE connections, or 1450 for PPTP connections. For some ISPs, you might need to reduce the MTU size, but this is rarely required and should not be done unless you are sure it is necessary for your ISP connection. For more information, see "Changing the MTU Size" on page 5-15.

To change the MTU size:

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

Configuring NAT Filtering

Network Address Translation (NAT) determines how the router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function. For more information about NAT, see "How Your Computer Accesses a Remote Computer through Your Router" on page 5-2.

To change the NAT option:

1. In the NAT Filtering area, select either the **Secured** or the **Open** radio button.
2. Click **Apply** to save the new configuration.

Configuring Static Routes

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

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

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 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 forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

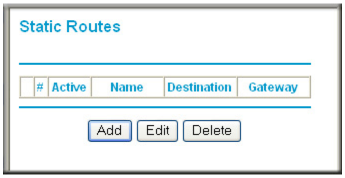
In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100.

In this example:

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** field specifies that all traffic for these addresses should be forwarded to the ISDN router at 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.

To add or edit a static route:

1. Select **Static Routes** under Advanced in the main menu. The Static Routes screen displays.

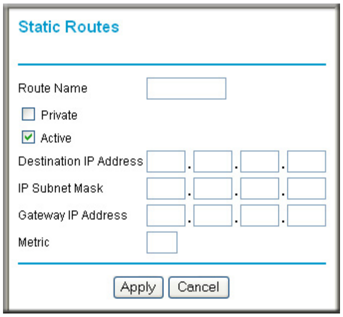


Static Routes

	#	Active	Name	Destination	Gateway

Figure 4-5

2. Click **Add** to expand the Static Routes screen.



Static Routes

Route Name

□ Private

☑ Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

Figure 4-6

3. In the **Route Name** field, enter a name for this static route. (This is for identification purposes only.)
4. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.
5. Select the **Active** check box to make this route effective.
6. In the **Destination IP Address** field, enter the IP address of the final destination.
7. In the **IP Subnet Mask** field, enter the IP subnet mask for this destination. If the destination is a single host, enter **255.255.255.255**.
8. In the **Gateway IP Address** field, enter the gateway IP address, which must be a router on the same LAN segment as the WNR1000 v2h2 router.
9. In the **Metric** field, enter 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.
10. Click **Apply** to have the static route entered into the table.

Chapter 5
Fine-Tuning Your Network

This chapter describes how to modify the configuration of the N 150 Wireless Router WNR1000 v2h2 to allow specific applications to access the Internet or to be accessed from the Internet, and how to make adjustments to enhance your network's performance.

This chapter includes the following sections:

- "Allowing Inbound Connections to Your Network"
- "Configuring Port Forwarding to Local Servers" on page 5-6
- "Configuring Port Triggering" on page 5-9
- "Using Universal Plug and Play" on page 5-12
- "Optimizing Wireless Performance" on page 5-14
- "Changing the MTU Size" on page 5-15
- "Overview of Home and Small Office Networking Technologies" on page 5-16

Allowing Inbound Connections to Your Network

By default, the WNR1000 v2h2 router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. However, you might need to create exceptions to this rule for the following purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when their replies are not recognized by your router.

Your router provides two features for creating these exceptions: port forwarding and port triggering. This section explains how a normal outbound connection works, followed by two examples explaining how port forwarding and port triggering operate and how they differ.

How Your Computer Accesses a Remote Computer through Your Router

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing source and destination address and process information. Before forwarding your message to the remote computer, your router must modify the source information and must create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open Internet Explorer, beginning a browser session on your computer. Invisible to you, your operating system assigns a service number (port number) to every communication process running on your computer. In this example, let's say Windows assigns port number 5678 to this browser session.
2. You ask your browser to get a Web page from the Web server at www.example.com. Your computer composes a Web page request message with the following address and port information:
   - The source address is your computer's IP address.
   - The source port number is 5678, the browser session.
   - The destination address is the IP address of www.example.com, which your computer finds by asking a DNS server.
   - The destination port number is 80, the standard port number for a Web server process.

   Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the Web server at www.example.com. Before sending the Web page request message to www.example.com, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):
   - The source address is replaced with your router's public IP address.
     This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
   - The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

   Your router then sends this request message through the Internet to the Web server at www.example.com.

4. The Web server at www.example.com composes a return message with the requested Web page data. The return message contains the following address and port information:
   - The source address is the IP address of www.example.com.
   - The source port number is 80, the standard port number for a Web server process.
   - The destination address is the public IP address of your router.
   - The destination port number is 33333.

   The Web server then sends this reply message to your router.
5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message, restoring the original address information replaced by NAT. The message now contains the following address and port information:
   - The source address is the IP address of www.example.com.
   - The source port number is 80, the standard port number for a Web server process.
   - The destination address is your computer's IP address.
   - The destination port number is 5678, the browser session that made the initial request.

   Your router then sends this reply message to your computer, which displays the Web page from www.example.com.
6. When you finish your browser session, your router eventually senses a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

How Port Triggering Changes the Communication Process

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router will not recognize it and will discard it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the port triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you must also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program, beginning a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.
3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule, and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, let's say port 33333) as the destination port. The IRC server also sends an "identify" message to your router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.
8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application, or user groups or newsgroups.

➡	**Note:** Only one computer at a time can use the triggered application.

How Port Forwarding Changes the Communication Process

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from our previous Web server example. In this case, a remote computer's browser needs to access a Web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a Web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens Internet Explorer and requests a Web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a Web page request message with the following destination information:
   - The destination address is the IP address of www.example.com, which is the address of your router.
   - The destination port number is 80, the standard port number for a Web server process.

   The remote computer then sends this request message through the Internet to your router.
2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:

   The destination address is replaced with 192.168.1.123.

   Your router then sends this request message to your local network.
3. Your Web server at 192.168.1.123 receives the request and composes a return message with the requested Web page data. Your Web server then sends this reply message to your router.
4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the Web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or user groups or newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- Port triggering does not need to know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address must never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Configuring Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might make a local Web server, FTP server, or game server visible and available to the Internet.

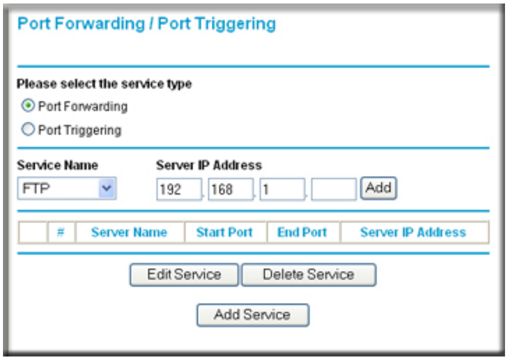
Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded. The DMZ server is configured in the WAN Setup screen, as discussed in "Setting Up a Default DMZ Server" on page 4-7.

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

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your WNR1000v2 router. See "Using Address Reservation" on page 4-4 for instructions on how to use reserved IP addresses.

To configure port forwarding to a local server:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu. The Port Forwarding/Port Triggering screen displays.



Port Forwarding / Port Triggering

Please select the service type

● Port Forwarding

○ Port Triggering

Service Name: FTP

Server IP Address: 192 . 168 . 1 .

	#	Server Name	Start Port	End Port	Server IP Address

Figure 5-1

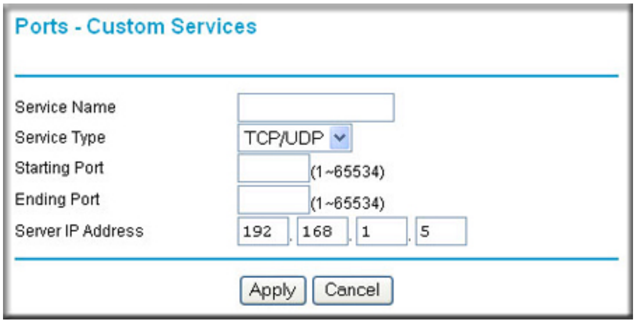
2. From the **Service Name** list, select the service or game that you will host on your network. If the service does not appear in the list, see the following section, "Adding a Custom Service."
3. In the corresponding **Server IP Address** fields, enter the last digit of the IP address of your local computer that will provide this service.
4. To the right of Server IP Address, click **Add**. The service appears in the list in the screen.

Adding a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you must first determine which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups. When you have the port number information, follow these steps:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu.

2. Click **Add Service** (see Figure 5-1 on page 5-7).The Ports–Custom Services screen displays.



Ports - Custom Services

Service Name	
Service Type	TCP/UDP
Starting Port	(1~65534)
Ending Port	(1~65534)
Server IP Address	192 . 168 . 1 . 5

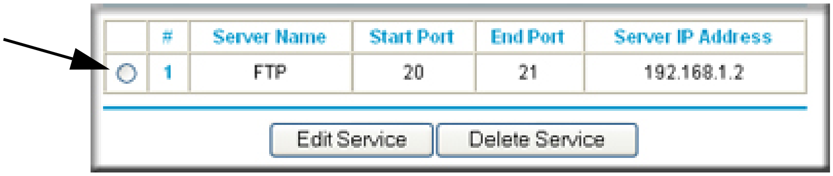
Figure 5-2

3. In the **Service Name** field, enter a descriptive name.
4. In the **Service Type** field, select the protocol. If you are unsure, select **TCP/UDP**.
5. In the **Starting Port** field, enter the beginning port number.
   - If the application uses only a single port, enter the same port number in the **Ending Port** field.
   - If the application uses a range of ports, enter the ending port number of the range in the **Ending Port** field.
6. In the **Server IP Address** field, enter the IP address of your local computer that will provide this service.
7. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Editing or Deleting a Port Forwarding Entry

To edit or delete a port forwarding entry:

1. In the table, select the button next to the service name.



	#	Server Name	Start Port	End Port	Server IP Address
○	1	FTP	20	21	192.168.1.2

Figure 5-3

2. Click **Edit Service** or **Delete Service** to make changes.
3. Click **Apply**.

Application Example: Making a Local Web Server Public

If you host a Web server on your local network, you can use port forwarding to allow Web requests from anyone on the Internet to reach your Web server.

To make a local Web server public:

1. Assign your Web server either a fixed IP address or a dynamic IP address using DHCP address reservation, as explained in "Using Address Reservation" on page 4-4. In this example, your router will always give your Web server an IP address of 192.168.1.33.
2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your Web server at **192.168.1.33**.
   HTTP (port 80) is the standard protocol for Web servers.
3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name as described in "Using a Dynamic DNS Service" on page 4-5.
   To access your Web server from the Internet, a remote user must know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Configuring Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound "trigger" port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

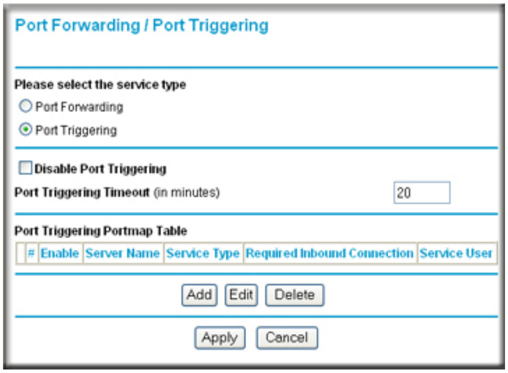
While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in "Using Universal Plug and Play" on page 5-12.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

To set up port triggering:

1. Select **Port Forwarding/Port Triggering** under Advanced in the main menu. The Forwarding/Port Triggering screen displays (see Figure 5-1 on page 5-7).
2. Select the **Port Triggering** radio button. The port triggering information displays.



Port Forwarding / Port Triggering

Please select the service type

○ Port Forwarding

● Port Triggering

□ Disable Port Triggering

Port Triggering Timeout (in minutes) 20

Port Triggering Portmap Table

#	Enable	Server Name	Service Type	Required Inbound Connection	Service User

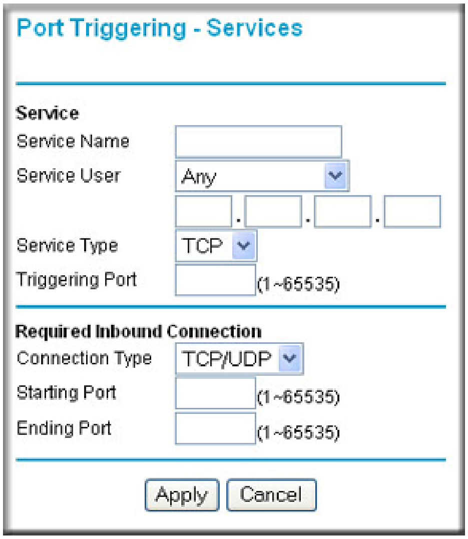
Figure 5-4

3. Clear the **Disable Port Triggering** check box.

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

4. In the **Port Triggering Timeout** field, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

5. Click **Add**. the Port Triggering–Services screen displays.



Port Triggering - Services

Service

Service Name

Service User: Any

Service Type: TCP

Triggering Port (1~65535)

Required Inbound Connection

Connection Type: TCP/UDP

Starting Port (1~65535)

Ending Port (1~65535)

Figure 5-5

6. In the **Service Name** field, enter a descriptive service name.

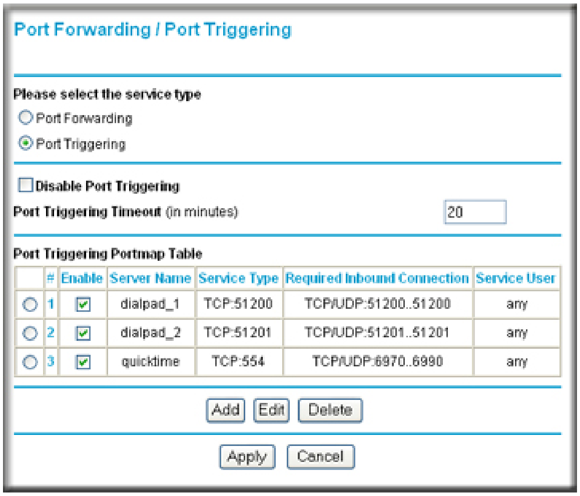
7. In the **Service User** field, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.

8. Select the service type, either **TCP** or **UDP**.

9. In the **Triggering Port** field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.

10. Enter the inbound connection port information in the **Connection Type**, **Starting Port**, and **Ending Port** fields.

11. Click **Apply**. The service appears in the Port Triggering Portmap table.



Port Forwarding / Port Triggering

Please select the service type

○ Port Forwarding

● Port Triggering

□ Disable Port Triggering

Port Triggering Timeout (in minutes) 20

Port Triggering Portmap Table

	#	Enable	Server Name	Service Type	Required Inbound Connection	Service User
○	1	☑	dialpad_1	TCP:51200	TCP/UDP:51200..51200	any
○	2	☑	dialpad_2	TCP:51201	TCP/UDP:51201..51201	any
○	3	☑	quicktime	TCP:554	TCP/UDP:6970..6990	any

Figure 5-6

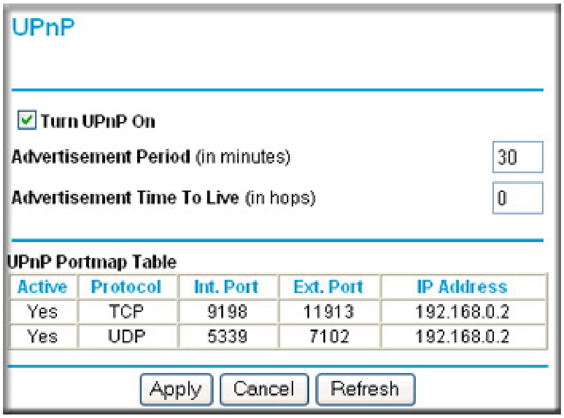
Using Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, to 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.

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

To turn on Universal Plug and Play:

1. Select **UPnP** under Advanced the main menu. The UPnP screen displays.



UPnP

☑ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time To Live (in hops) 0

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
Yes	TCP	9198	11913	192.168.0.2
Yes	UDP	5339	7102	192.168.0.2

Figure 5-7

2. The available settings and information displayed in this screen are:
    - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If this check box is not selected, the router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the router.
    - **Advertisement Period**. The advertisement period is how often the router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.
    - **Advertisement Time To Live**. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. 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 might be necessary to increase this value.
    - **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 whether that port is still active for each IP address.
3. Click **Apply** to save your settings.