

NETGEAR 54 Mbps Wireless Router WGR614v8 Reference Manual



NETGEAR®

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

202-10226-01
July 2007

Trademarks

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

Product Registration and Customer Support

Register your product at <http://www.netgear.com/support>. Registration is required before you can use our telephone support service. For specific product support information, refer to the Support Information Card included with your Router Model WGR614v8.

When the wireless router is connected to the Internet, additional information is provided by clicking either the Knowledge Base link or the Documentation link under the Web Support menu. The KnowledgeBase link provides product support information and the Documentation link directs you to the documentation for the wireless router.

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.

Wireless Communications

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

FCC Statement

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 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.

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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.










The radio module has been evaluated under FCC Bulletin OET 65C (01-01) and found to be compliant to the requirements as set forth in CFR 47 Sections, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. This model meets the applicable government requirements for exposure to radio frequency waves.

Europe – EU Declaration of Conformity

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

EN300 328, EN301 489-17, EN60950-1

Europe – Declaration of Conformity in Languages of the European Community

 Český [Czech]	<i>NETGEAR Inc.</i> tímto prohlašuje, že tento Radiolan je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>NETGEAR Inc.</i> erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erkläre <i>NETGEAR Inc.</i> , dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>NETGEAR Inc.</i> seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>NETGEAR Inc.</i> , declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>NETGEAR Inc.</i> declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ἑλληνικά [Greek]	Ἡ ἘΤΕΡΑ ἘΜΠΡΟΣΩΠΕΙ ΤΗΝ <i>NETGEAR Inc.</i> Ἡ ἘΤΕΡΑ ἘΚΔΕΛΦΕΤΙ Τὸ ἘΠΙΧΕΙΡΗΣΙΟ ΤΟΥ ΡΑΔΙΟΛΑΝ ὅτι συμμορφώνεται μετὰ τὰς ἐσσημειωθεὶς ἀπὸ τῆς Ἐπιτροπῆς τῆς Ἐνωσης τῶν Κρατῶν τῆς Ἐξουχίας τῆς Ἐνέργειας 1999/5/ἘΕ.
 Français [French]	Par la présente <i>NETGEAR Inc.</i> déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>NETGEAR Inc.</i> dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

[lv] Latviski [Latvian]	Ar šo <i>NETGEAR Inc.</i> deklarāc, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[lt] Lietuvių [Lithuanian]	Šiuo <i>NETGEAR Inc.</i> deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[nl] Nederlands [Dutch]	Hierbij verklaart <i>NETGEAR Inc.</i> dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
[mt] Malti [Maltese]	Hawnhekk, <i>NETGEAR Inc.</i> , jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
[hu] Magyar [Hungarian]	Alulírott, <i>NETGEAR Inc.</i> nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
[pl] Polski [Polish]	Niniejszym <i>NETGEAR Inc.</i> oświadczam, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[pt] Português [Portuguese]	<i>NETGEAR Inc.</i> declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
[sl] Slovensko [Slovenian]	<i>NETGEAR Inc.</i> izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
[sk] Slovensky [Slovak]	<i>NETGEAR Inc.</i> týmto vyhlasuje, že Radiolan spáda základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
[fi] Suomi [Finnish]	<i>NETGEAR Inc.</i> vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[sv] Svenska [Swedish]	Härmed intygar <i>NETGEAR Inc.</i> att denna Radiolan står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir <i>NETGEAR Inc.</i> yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
[no] Norsk [Norwegian]	<i>NETGEAR Inc.</i> erklærer herved at utstyret <i>Radiolan</i> er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Router Model WGR614v8 gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

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

Certificate of the Manufacturer/Importer

It is hereby certified that the Router Model WGR614v8 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

MIC Compliance, “Class B” Equipment (Household purpose info/telecommunications equipment)

As this equipment has undergone EMC registration for household purposes, this product can be used in any area including residential areas.

Product and Publication Details

Model Number:	WGR614v8
Publication Date:	July 2007
Product Family:	Product Family
Product Name:	Router Model WGR614v8
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10226-01

Contents

About This Manual

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

Chapter 1

Introduction

Key Features	1-1
802.11g Wireless Networking	1-2
A Powerful, True Firewall with Content Filtering	1-2
Security	1-3
Autosensing Ethernet Connections with Auto Uplink	1-3
Extensive Protocol Support	1-3
Easy Installation and Management	1-4
Maintenance and Support	1-5
Package Contents	1-5
The Router Front Panel	1-5
The Router Back Panel	1-7
Default Factory Settings	1-8

Chapter 2

Internet and Wireless Settings

Installing Your Router Using the Smart Wizard	2-1
Logging Into Your Router	2-1
Changing Your Configuration	2-5
Internet Settings	2-5
Wireless Security Settings	2-8
Accessing the Router After Installation	2-11
Placement of the Router to Optimize Wireless Connectivity	2-12

Chapter 3

Content Filtering

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

Chapter 4

Maintenance

Viewing Wireless Router Status Information	4-1
Viewing a List of Attached Devices	4-5
Configuration File Management	4-5
Restoring and Backing Up the Configuration	4-6
Erasing the Configuration	4-7
Upgrading the Router Software	4-7
Changing the Administrator Password	4-9

Chapter 5

Advanced Router Configuration

Setting up a Vista WPS Network	5-1
Configuring Port Triggering	5-3
Configuring Port Forwarding to Local Servers	5-6
Adding a Custom Service	5-7
Editing or Deleting a Port Forwarding Entry	5-8
Local Web and FTP Server Example	5-8
Multiple Computers for Half Life, KALI or Quake III Example	5-8
Configuring the WAN Setup Options	5-9
Disabling the SPI Firewall	5-9
Setting Up a Default DMZ Server	5-10
Responding to Ping on Internet WAN Port	5-10
Setting the MTU Size	5-10
NAT Filtering	5-11
Using the LAN IP Setup Options	5-11

Configuring LAN TCP/IP Setup Parameters	5-12
Using the Router as a DHCP server	5-13
Using Address Reservation	5-13
Using a Dynamic DNS Service	5-14
Configuring Static Routes	5-16
Enabling Remote Management Access	5-18
Using Universal Plug and Play (UPnP)	5-20

Chapter 6

Troubleshooting

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

Appendix A

Technical Specifications

Appendix B

Related Documents

About This Manual

The *NETGEAR® 54 Mbps Wireless Router WGR614v8 Reference Manual* describes how to install, configure and troubleshoot the Router Model WGR614v8. The information in this manual is intended for readers with intermediate computer and Internet skills.

Conventions, Formats and Scope


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


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


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

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

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

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


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

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

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






Product Version	Router Model WGR614v8
Manual Publication Date	July 2007

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

	Note: Product updates are available on the NETGEAR, Inc. Web site at http://kbserver.netgear.com/products/WGR614v8.asp
---	---

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print this Manual

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

- **Printing a Page from HTML.** Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents.
- **Printing from PDF.** Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at <http://www.adobe.com>.
 - **Printing a PDF Chapter.** Use the *PDF of This Chapter* link at the top left of any page.

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



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

Part Number	Version Number	Date	Description
202-10226-01	1.0	July 2007	<ul style="list-style-type: none">• Remove Trend Micro• Add Vista WPS advanced features

Chapter 1

Introduction

Congratulations on your purchase of the NETGEAR® Router Model WGR614v8. The Wireless Router provides connection for multiple computers to the Internet through an external broadband access device (such as a cable modem or DSL modem) that is normally intended for use by a single computer. This chapter describes the features of the NETGEAR Router Model WGR614v8.

Key Features

The Router Model WGR614v8 with 4-port switch connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The Wireless Router provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Web site addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253 computers. In addition to the Network Address Translation (NAT) feature, the built-in firewall protects you from hackers.

With minimum setup, you can install and use the router within minutes.

The Wireless Router provides the following features:

- 802.11g wireless networking, with the ability to operate in 802.11 b-only, 802.11g-only, or 802.11b+g modes.
- Easy, Web-based setup for installation and management.
- Content Filtering and Site Blocking Security.
- Built in 4-port 10/100 Mbps Switch.
- Ethernet connection to a wide area network (WAN) device, such as a cable modem or DSL modem.
- Extensive Protocol Support.
- Login capability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrades.

802.11g Wireless Networking

The Wireless Router includes an 802.11g wireless access point, providing continuous, high-speed 54 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11g wireless networking at up to 54 Mbps.
- 802.11g wireless networking, with the ability to operate in 802.11g-only, 802.11b-only, or 802.11g and b modes, providing backwards compatibility with 802.11b devices or dedicating the wireless network to the higher bandwidth 802.11g devices.
- 64-bit and 128-bit WEP encryption security.
- WEP keys can be generated manually or by passphrase.
- WPA-PSK and WPA2-PSK support. Support for Wi-Fi Protected Access (WPA) data encryption which provides strong data encryption and authentication based on a pre-shared key.
- Wireless access can be restricted by MAC address.
- Wireless network name broadcast can be turned off so that only devices that have the network name (SSID) can connect.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the WGR614v8 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection.
Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents.

The WGR614v8 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to E-mail the log to you at specified intervals. You can also configure the router to send immediate alert messages to your E-mail address or E-mail pager whenever a significant event occurs.

- The WGR614v8 prevents objectionable content from reaching your computers. The router allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the router to log and report attempts to access objectionable Internet sites.

Security

The Wireless Router is equipped with several features designed to maintain security, as described in this section.

- **Computers Hidden by NAT**
NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the computers on the LAN.
- **Port Forwarding with NAT**
Although NAT prevents Internet locations from directly accessing the computers on the LAN, the router allows you to direct incoming traffic to specific computers based on the service port number of the incoming request, or to one designated “DMZ” host computer. You can specify forwarding of single ports or ranges of ports.

Autosensing Ethernet Connections with Auto Uplink

With its internal 4-port 10/100 switch, the WGR614v8 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The router incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a “normal” connection such as to a computer or an “uplink” connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Extensive Protocol Support

The Wireless Router supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to [Appendix B, “Related Documents”](#).

- **IP Address Sharing by NAT**

The Wireless Router allows several networked computers to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.

- **Automatic Configuration of Attached computers by DHCP**

The Wireless Router dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached computers on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of computers on your local network.

- **DNS Proxy**

When DHCP is enabled and no DNS addresses are specified, the router provides its own address as a DNS server to the attached computers. The router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.

- **PPP over Ethernet (PPPoE)**

PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as Entersys or WinPOET on your computer.

Easy Installation and Management

You can install, configure, and operate the Router Model WGR614v8 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**

Browser-based configuration allows you to easily configure your router from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.

- **Smart Wizard**

The Wireless Router Smart Wizard automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.

- **Windows Connect Now**

If connecting from a Windows Vista Machine, you can use Windows Connect Now to implement WPS (Wi-Fi Protected Setup) and configure the SSID (device name) and WPA security password for your router.

- **Firmware Update**

The Wireless Router can be updated if a newer version of firmware is available. This lets you take advantage of product enhancements for your WGR614v8 as soon as they become available.

- **Visual monitoring**

The Wireless Router's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the Wireless Router:

- Flash memory for firmware upgrades.
- Free technical support seven days a week, twenty-four hours a day, for 90 days from the date of purchase.

Package Contents

The product package should contain the following items:

- Router Model WGR614v8.
- AC power adapter.
- Vertical stand.
- Category 5 (CAT5) Ethernet cable.
- *Resource CD*, including:
 - This guide.
 - The Installation Guide.
 - Application Notes and other helpful information..
- Registration, Warranty Card, and Support Information Card.

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

The Router Front Panel

The front panel of the Wireless Router contains the status lights described below.

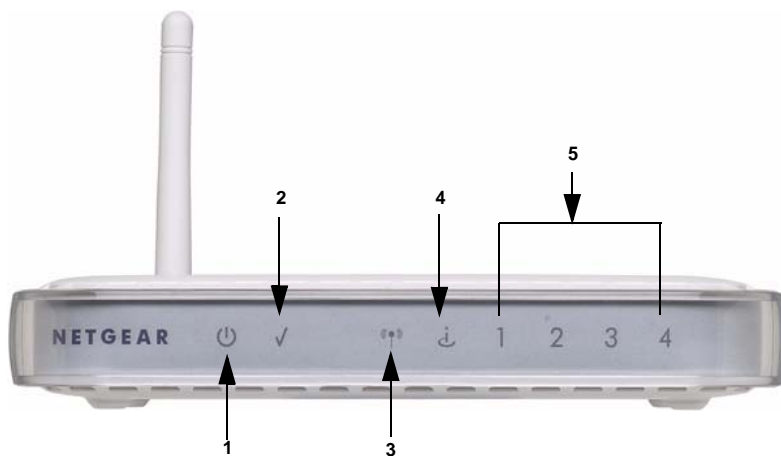


Figure 1-1

You can use the status lights to verify connections.

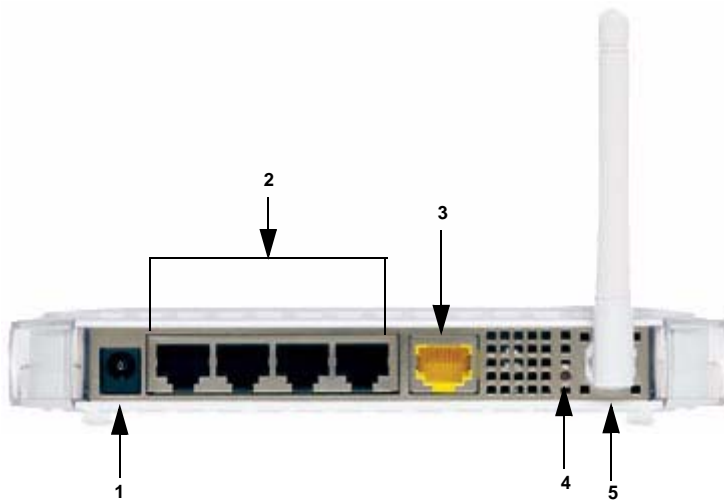
Table 1-1. Status Light Descriptions

Label	Activity	Description
1. Power	On Blink Off	Power is supplied. Firmware is corrupt; the router is in rescue mode running TFTP server. Users can use TFTP client to upload a valid version of the firmware. Power is not supplied to the router.
2. Test	On Blink Off	The unit is performing the power on self test diagnostic. The unit is performing a firmware upgrade or restoring the factory defaults. The unit successfully completed the power on self test diagnostic.
3. Wireless	On Off	The Wireless port is initialized and the wireless feature is enabled. The wireless feature is turned off or there is a problem.
4. Internet	On (amber) On (green) Blink (green)	The ethernet cable is connected but the router has not received an Internet address. The router has received an Internet address. Data is being transmitted or received by the Internet port.

Table 1-1. Status Light Descriptions (continued)

Label	Activity	Description
5. LAN	On (green)	The LAN (local area network) port has detected link with a 100 Mbps device.
	Blink (green)	Data is being transmitted or received at 100 Mbps.
	On (amber)	The Local port has detected link with a 10 Mbps device.
	Blink (amber)	Data is being transmitted or received at 10 Mbps.
	Off	No link is detected on this port.

The Router Back Panel

**Figure 1-2**

The back panel of the WGR614v8 router contains the following port connections:

1. Power adapter port
2. Four local Ethernet ports for connecting the local computers
3. Internet port for connecting to a cable or ADSL modem
4. Factory default reset button
5. Wireless antenna

Default Factory Settings

When you first receive your WGR614v8, the default factory settings are set as shown in [Appendix A, “Technical Specifications.”](#) If you change the settings, you can restore these defaults with the Factory Default Restore button on the rear panel. After you install the Wireless Router, use the procedures in the following chapters to customize any of the settings to better meet your networking needs.

Chapter 2

Internet and Wireless Settings

This chapter describes how to use the Smart Wizard Installation Assistant on the Resource CD to configure your wireless router's Internet connection and wireless parameters.

Once you are connected to the Internet and your wireless connections are working, you can also configure the router's content filtering parameters if you need to change the default settings. See [Chapter 3, "Content Filtering"](#).

If you are an advanced user, you can also configure maintenance (see [Chapter 4, "Maintenance"](#)) and advanced (see [Chapter 5, "Advanced Router Configuration"](#)) settings if you need to change the factory defaults.



Note: Do not change your existing Internet connection. Instead, let the Smart Wizard Installation Assistant on the Resource CD guide you through the setup process.

Installing Your Router Using the Smart Wizard

1. Insert the Resource CD into the CD drive on your PC.
2. Click Setup and follow the instructions. The Smart Wizard Installation Assistant will guide you through the setup process:
 - How to change your cabling.
 - How to connect to the Internet.
 - How to configure your wireless settings.

If you want to change your Internet or wireless settings later, see ["Changing Your Configuration" on page 2-5](#).

Logging Into Your Router


To log into your router after you have configured your router, do the following:

1. Type <http://www.routerlogin.net> in the address field of Internet Explorer or Netscape® Navigator.



Figure 2-1

2. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters (or enter the password you chose if you changed it during the setup in [“Installing Your Router Using the Smart Wizard”](#) on page 2-1).

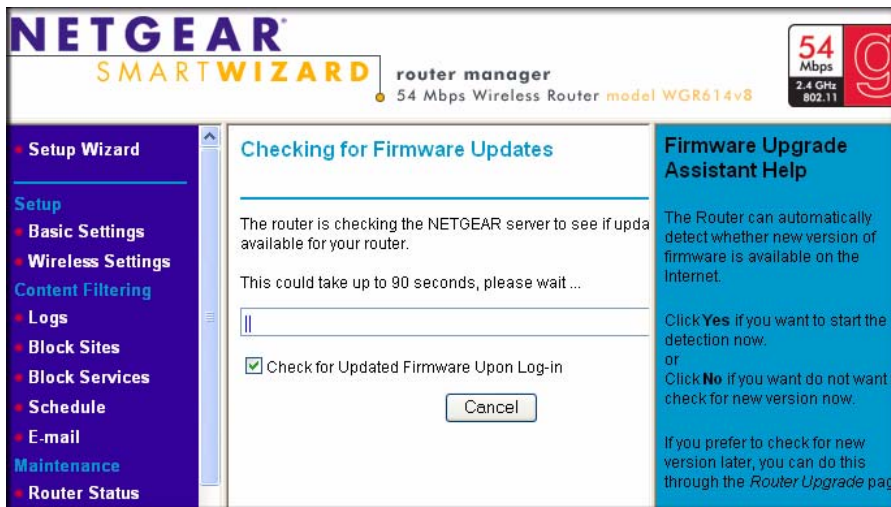
	Note: The router user name and password are not the same as any user name or password you may use to log in to your Internet connection.
---	---

A login window like the one shown below opens:

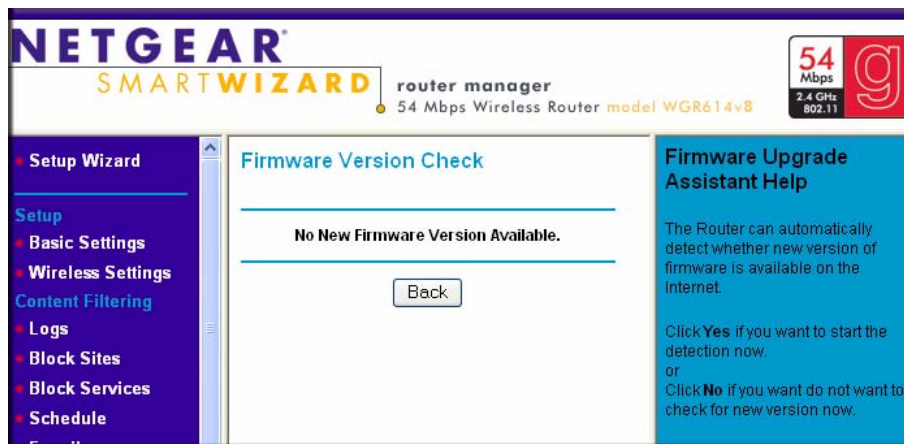


Figure 2-2

3. Click OK. The Checking for Firmware Updates screen will display.

**Figure 2-3**

Your router will automatically check the NETGEAR firmware server for new firmware. If new firmware is available, you will be asked if you want to update your router (see [“Upgrading the Router Software”](#) on page 4-7). If no new firmware is available, the following screen will display.

**Figure 2-4**

4. Select Basic Settings from under the Setup menu. The Basic Settings screen will display showing the default settings of your router.

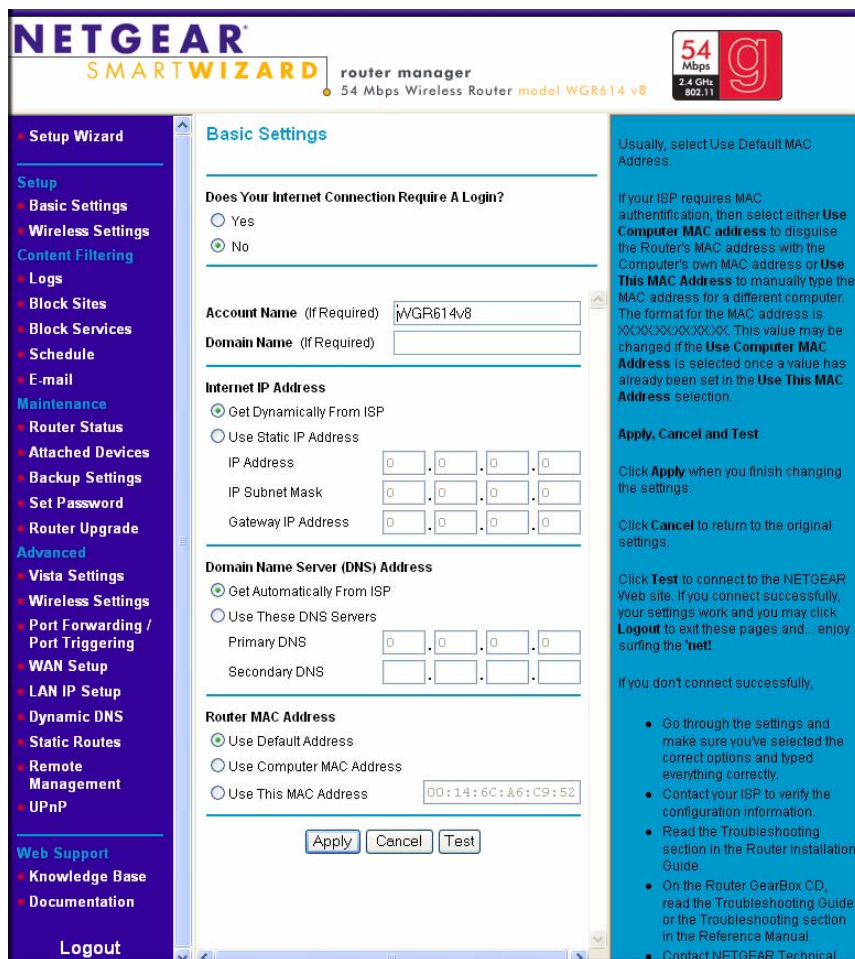


Figure 2-5

The router menu screens allow you to configure, upgrade and check the status of your NETGEAR Wireless Router.

Select an item from the menu on the left of the screen. The current settings or information about that area will appear in the center column.

Helpful information related to the settings for the selected screen appear in this column. If you are using Internet Explorer, you may click on an item in the center column which will take you to the related help section located on the right of the screen; you may also scroll down the screen to access additional information.

For current product support information and product firmware upgrades, go to:
<http://kbserver.netgear.com/products/WGR614v8.asp>

Changing Your Configuration

You can change your Internet and wireless settings after they have been configured by the Smart Wizard Configuration Assistant.

Internet Settings

To change the Internet settings:

1. Select Setup > Basic Settings from the menu on the left. The screen on the left will appear:

Basic Settings, 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
 IP Subnet Mask
 Gateway IP Address

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

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

Basic Settings, Login Required

Basic Settings

Does Your Internet Connection Require A Login?
 Yes
 No

Internet Service Provider

Login
 Password

Service Name (If Required)

Connection Mode

Idle Timeout (In Minutes)

Internet IP Address
 Get Dynamically From ISP
 Use Static IP Address

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

Figure 2-6



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

2. Enter the following information based on your connection type:

- **Does Your Internet Connection Require A Login?:** Select this option based on the type of account you have with your ISP. If you need to enter login information every time you connect to the Internet or you have a PPPoE account with your ISP, select Yes. Otherwise, select No.



Note: If you have installed PPP software such as WinPoET (from Earthlink) or Enternet (from PacBell), then you have PPPoE. Select Yes. After selecting Yes and configuring your router, you will not need to run the PPP software on your PC to connect to the Internet.

• If you selected the **Yes** radio box:

- Enter your **Internet Service Provider**. Select the service provided by your ISP. “Other” (PPPoE) is the most common. “PPTP” is used in Austria and other European countries. “Telstra BigPond” is for Australia only. Then, enter the information in the following fields:
 - **Login:** This is usually the name that you use in your e-mail address. For example, if your main mail account is JerAB@ISP.com, then put JerAB in this box. Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full e-mail address when you log in. If your ISP requires your full e-mail address, then type it in the Login box.
 - **Password:** Type the password that you use to log in to your ISP.
 - **Service Name** (if required): If your ISP provided a Service Name, enter it here. Otherwise, this may be left blank.
 - **Connection Mode:** Set the Connection Mode to one of the following:
 - **Dial on Demand** (default setting) – A PPOE/PPTP/BigPond connection automatically starts when there is outbound traffic to the Internet, and the connection automatically terminates if the connection is idle based on the value in the Idle Timeout setting.
 - **Always On** – A PPOE/PPTP/BigPond connection automatically starts when the computer boots up, but the connection does not time out. The router will keep trying to bring up the connection if it is disconnected for some reason.

- **Manually Connect** – You must go to the Router Status screen and click the Connect button in order to connect to the Internet. The manual connection does not time out and you must click the Disconnect button on the Router Status screen to disconnect the router.
- **Idle Timeout:** An idle Internet connection will be terminated after this time period. If this value is zero (0), then the connection will be “kept alive” by re-connecting immediately whenever the connection is lost.
- If you selected the **No** radio box, enter the following information (if required):
 - **Account Name** (also called the Host Name of System Name). For most users, this is your account name or user name. For example, if your main account is JSmith@ISP.com, then enter JSmith in this field. If your ISP has given you a specific Host Name, then enter that name in the Account Name field.
 - Domain Name. Unless required by your ISP, you may leave this field blank. Some ISPs require the domain name of the ISP be entered in this field; for example, if the ISP mail server is mail.xxx.yyy.zzz, you would enter that name in the Domain Name field.
- **Internet IP Address:**
 - If you log in to your service or your ISP did not provide you with a fixed IP address, the router will find an IP address for you automatically when you connect. Select the **Get Dynamically from ISP** radio box.
 - If you have a fixed (static, permanent) IP address, your ISP will have provided you with an IP address. Select **Use Static IP Address** and enter the IP Address in the fields provided.
For example:
IP Address: 24.218.156.183
Subnet Mask: 255.255.255.0
Gateway IP Address: 24.218.156.1
- **Domain Name Server (DNS) Address:** The DNS server is used to look up site addresses based on their names.
 - Select **Get Automatically From ISP** if your ISP has not provided DNS addresses.

- If your ISP gave you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses.



Note: If you get “Address not found” errors when you go to a Web site, it is likely that your DNS servers aren’t set up properly. You should contact your ISP to get DNS server addresses.

- **Router MAC Address:** Your computer’s local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address.
 - Select **Use Default Address**, which is the router’s MAC address, unless your ISP requires authentication.
 - If your ISP requires MAC authentication, then you can select either
 - **Use Computer MAC Address** to disguise the router’s MAC address with the by using the computer’s own MAC address, or
 - **Use This MAC Address** and manually enter the MAC address for a different computer. The format for the MAC address is XX:XX:XX:XX:XX:XX. (This value may be changed if the Use Computer MAC Address is selected once a value has already been set in the Use This MAC Address selection.)
- 3. Click **Test** to connect to the NETGEAR Web site. If you connect successfully, your settings work and you may click **Logout** to exit router interface.

If you don't connect successfully,

1. Go through the settings and make sure you've selected the correct options and typed everything correctly.
2. Contact your ISP to verify the configuration information.
3. Read the Troubleshooting section in the Router Installation Guide.
4. On the Router Resource CD, read the Troubleshooting Guide or see [“Troubleshooting.”](#)
5. Contact NETGEAR Technical Support.

Wireless Security Settings

To change the wireless settings:

1. Select Setup > Wireless Settings from the menu on the left. The Wireless Settings screen will display.

Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: Auto

Mode: b and g

Security Options

None

WEP

WPA-PSK [TKIP]

WPA2-PSK [AES]

WPA-PSK [TKIP] + WPA2-PSK [AES]

Apply Cancel

Figure 2-7

2. Enter a **Name (SSID)** in the field provided with a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is NETGEAR, but NETGEAR strongly recommends that you change your network's Name (SSID) to a different value. This value is also case-sensitive. For example, NETGEAR is not the same as NETGEAR.
- Select your region from the **Region** drop-down menu. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency or check our web site for more information on which channels to use.
3. Select a channel from the **Channel** drop-down menu (Auto is the default). This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.
4. Select the desired wireless mode from the **Mode** drop-down menu. The options are:
 - **b and g**: Both 802.11g and 802.11b wireless stations can be used.
 - **g only**: Only 802.11g wireless stations can be used.

The default is “b and g”, which allows both “b” and “g” wireless stations to access this device.



Note: To ensure proper agency compliance and compatibility between similar products in your area; the operating channel and region must be set correctly.

- Select your **Security Options** by checking the appropriate radio button. The various Security options are described below.

No Security

WEP Security

WPA-PSK Security

WPA2-PSK Security

WPA-PSK+WPA2-PSK

Figure 2-8

- **None:** No data encryption
- **WEP (Wired Equivalent Privacy):** Uses WEP 64 or 128 bit data encryption. If selected, enter the following information.
 - **Authentication Type:** From the pull-down menu, select Automatic (the default), Open System or Shared Key. Check your wireless card's documentation to see what method to use.
 - **Encryption Strength:** From the pull-down menu, select either 64-bit (sometimes called 40-bit) encryption or 128-bit encryption.
 - **Automatic Key Generation (Passphrase):** You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network. Enter a word or group of printable characters in the Passphrase box and click the Generate button to automatically configure the WEP Key(s). If encryption strength is set to 64 bit, then each of the four key boxes will automatically be populated with 10 hexadecimal digits for the key values. If encryption strength is set to 128 bit, then 26 hexadecimal digits will be selected for the key values. Check the radio box for the key that will be used.
- **WPA-PSK [TKIP]** – Wi-Fi Protected Access with Pre-Shared Key; use WPA-PSK standard encryption with TKIP encryption type by entering a group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters.
- **WPA2-PSK [AES]** – Wi-Fi Protected Access version 2 with Pre-Shared Key; use WPA2-PSK standard encryption with the AES encryption type by entering a group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters.
- **WPA-PSK [TKIP] + WPA2-PSK [AES]** – Allows clients access using either WPA-PSK [TKIP] or WPA2-PSK [AES].

Accessing the Router After Installation

You can access the router after installation to modify or change any settings. To access the router after setup:

1. In your browser window, enter **http://www.routerlogin.net** or **192.168.1.1**.
2. When the log in screen appears, enter the default user name **admin** and password **password**, or whatever user name and password you selected when you initially set up your router. Click Apply.

3. The Checking for New Firmware screen will display. If you want to bypass this screen, click Cancel. The router Basic Settings screen will display.

If you do not click Logout, the wireless router waits for 5 minutes of no activity before it automatically logs you out.

Placement of the Router to Optimize Wireless Connectivity

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the router. For best results, place your router:

- Near the center of the area in which your PCs will operate
- In an elevated location such as a high shelf
- Away from potential sources of interference, such as PCs, microwaves, and cordless phones
- With the Antenna tight and in the upright position
- Away from large metal surfaces



Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

Chapter 3

Content Filtering

This chapter describes how to use the content filtering features of the Router Model WGR614v8 to protect your network. These features can be found by clicking on the Content Filtering heading in the Main Menu of the browser interface.

Content Filtering Overview

The Router Model WGR614v8 provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time of day, Web addresses and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

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

Blocking Access to Internet Sites

The Wireless Router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is shown in [Figure 3-1](#) below:

Block Sites

Keyword Blocking

Never
 Per Schedule
 Always

Type Keyword or Domain Name Here.

Add Keyword

Block Sites Containing these Keywords or Domain Names:

Delete Keyword Clear List

Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address 192 . 168 . 1 . 0

Apply Cancel

Figure 3-1

To enable keyword blocking, select either “Per Schedule” or “Always”, then click Apply. If you want to block by schedule, be sure that a time period is specified in the Schedule menu.

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

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

Keyword application examples:

- If the keyword “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
- If you wish to block all Internet browsing access during a scheduled period, enter the keyword “.” and set the schedule in the Schedule menu.

To specify a Trusted User, enter that PC’s IP address in the Trusted User box and click Apply.

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

Blocking Access to Internet Services

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

Block Services

Services Blocking

Never
 Per Schedule
 Always

Service Table

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

Add Edit Delete

Apply Cancel

Figure 3-2

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

To enable service blocking, select either Per Schedule or Always, then click Apply. If you want to block by schedule, be sure that a time period is specified in the Schedule menu.

To specify a service for blocking, click Add. The Add Services menu will appear, as shown below:

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: . . .

IP Address Range: to

All IP Addresses

Add Cancel

Figure 3-3

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

Configuring a User Defined Service

To define a service, first you must determine which port number or range of numbers is used by the application. The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, “Assigned Numbers.” Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application. This information can usually be determined by contacting the publisher of the application or from user groups or news groups.

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

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

Configuring Services Blocking by IP Address Range

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

Scheduling When Blocking Will Be Enforced

The Wireless Router allows you to specify when blocking will be enforced. The Schedule menu is shown below:

The screenshot shows a web-based configuration page titled "Schedule". It is divided into two main sections. The first section, "Days To Block:", contains a list of days from Sunday to Saturday, each with a checked checkbox. The second section, "Time Of Day To Block: (use 24-hour clock)", has a checked checkbox for "All Day". Below this, there are two rows of input fields: "Start Blocking:" and "End Blocking:", each with "Hour" and "Min" sub-labels and numeric input boxes. At the bottom of the form are "Apply" and "Cancel" buttons.

Figure 3-4

- Use this schedule for blocking content. Check this box if you wish to enable a schedule for Content Filtering. Click Apply.
- Days to Block. Select days to block by checking the appropriate boxes. Select Everyday to check the boxes for all days. Click Apply.
- Time of Day to Block. Select a start and end time in 23:59 format. Select All day for 24 hour blocking. Click Apply.

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

Viewing Logs of Web Access or Attempted Web Access

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

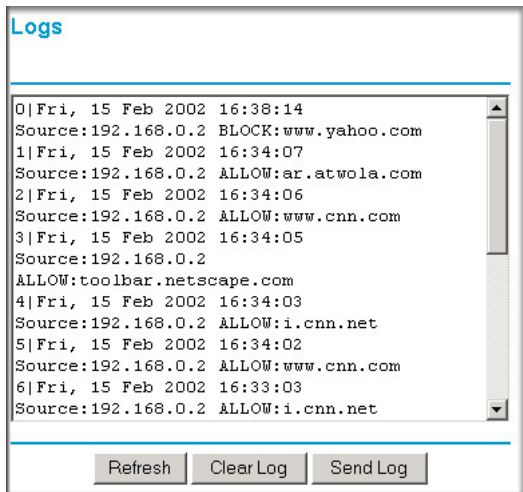


Figure 3-5

Log entries are described in [Table 3-1](#)

Table 3-1. Log entry descriptions

Field	Description
Number	The index number of the content filter log entries. 128 entries are available numbered from 0 to 127. The log will keep the record of the latest 128 entries.
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.
Action	This field displays whether the access was blocked or allowed.
	The name or IP address of the Web site or newsgroup visited or attempted to access.

Log action buttons are described in [Table 3-2](#)

Table 3-2. Log action buttons

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

Configuring E-Mail Alert and Web Access Log Notifications

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

E-mail

Turn E-mail Notification On

Send Alerts and Logs Via E-mail

Your Outgoing Mail Server: mail.myisp.com

Send To This E-mail Address: jsmith@myisp.com

My Mail Server requires authentication

User Name: john smith

Password: ●●●●●●●●

Send Alert Immediately

When Someone Attempts To Visit A Blocked Site.

Send Logs According to this Schedule

Weekly

Day: Sunday

Time: 12:00 a.m. p.m.

Time Zone

(GMT-08:00) Pacific Time (US Canada)

Automatically Adjust for Daylight Savings Time

Current Time: Wednesday, 01 Jan 2003 00:46:12

Apply Cancel

Figure 3-6

- Turn e-mail notification on
Check this box if you wish to receive e-mail logs and alerts from the router.
- Your outgoing mail server
Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.
- Send to this e-mail address
Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.
- My Mail server requires authentication.
If your e-mail server requires authentication, check this box.
- User Name
Enter the user name required by your mail server.
- Password
Enter the password required by your mail server.

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

- Send alert immediately
Check this box if you would like immediate notification of attempted access to a blocked site.
- Send logs according to this schedule
Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
 - Day for sending log
Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
 - Time for sending log
Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

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

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

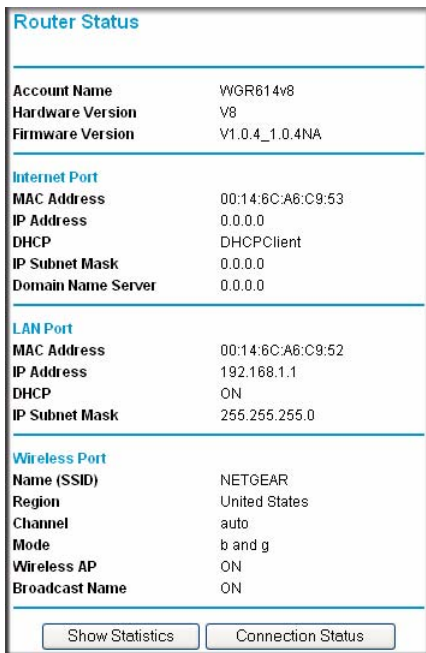
- **Time Zone**
Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
- **Daylight Savings Time**
Check this box if your time zone is currently under daylight savings time.

Chapter 4 Maintenance

This chapter describes how to use the maintenance features of your Router Model WGR614v8. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

Viewing Wireless Router Status Information

The Router Status menu provides status and usage information. From the Main Menu of the browser interface, select Maintenance > Router Status to view the System Status screen, shown below.



Router Status	
Account Name	WGR614v8
Hardware Version	V8
Firmware Version	V1.0.4_1.0.4NA
Internet Port	
MAC Address	00:14:6C:A6:C9:53
IP Address	0.0.0.0
DHCP	DHCPClient
IP Subnet Mask	0.0.0.0
Domain Name Server	0.0.0.0
LAN Port	
MAC Address	00:14:6C:A6:C9:52
IP Address	192.168.1.1
DHCP	ON
IP Subnet Mask	255.255.255.0
Wireless Port	
Name (SSID)	NETGEAR
Region	United States
Channel	auto
Mode	b and g
Wireless AP	ON
Broadcast Name	ON

Buttons: Show Statistics, Connection Status

Figure 4-1

This screen shows the following parameters:

Table 4-1. Wireless Router Status Fields

Field		Description
Account Name		This field displays the Host Name assigned to the router.
Hardware Version		This field displays the hardware version of the router.
Firmware Version		This field displays the current router firmware version.
Internet Port		These parameters apply to the Internet (WAN) port of the router.
	MAC Address	This field displays the Media Access Control address being used by the Internet (WAN) port of the router.
	IP Address	This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet.
	DHCP	If set to None, the router is configured to use a fixed IP address on the WAN. If set to Client, the router is configured to obtain an IP address dynamically from the ISP.
	IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router.
	DNS	This field displays the Domain Name Server addresses being used by the router.
LAN Port		These parameters apply to the Local (LAN) port of the router.
	MAC Address	This field displays the Media Access Control address being used by the LAN port of the router.
	IP Address	This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.1.1
	IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0
	DHCP	Identifies if the router's built-in DHCP server is active for the LAN attached devices.

Table 4-1. Wireless Router Status Fields (continued)

Field	Description
Wireless Port	These parameters apply to the Wireless port of the router.
MAC Address	This field displays the Media Access Control address being used by the Wireless port of the router.
Name (SSID)	This field displays the wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR.
Region	This field displays the geographic region where the router being used. It may be illegal to use the wireless features of the router in some parts of the world.
Channel	Identifies the channel of the wireless port being used. See “Wireless Communications” in Appendix B, “Related Documents” for the frequencies used on each channel.

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

IP Address	10.1.0.44
Subnet Mask	255.255.254.0
Default Gateway	10.1.1.13
DHCP Server	10.1.1.6
DNS Server	10.1.1.6 10.1.1.56
Lease Obtained	1 days,0 hrs,0 minutes
Lease Expires	0 days,23 hrs,55 minutes
<input type="button" value="Release"/> <input type="button" value="Renew"/>	
<input type="button" value="Close Window"/>	

Figure 4-2

This screen shows the following statistics:

Table 4-2: Connection Status Items

Item	Description
IP Address	The WAN (Internet) IP Address assigned to the router.
Subnet Mask	The WAN (Internet) Subnet Mask assigned to the router.

Table 4-2: Connection Status Items (continued)

Item	Description
Default Gateway	The WAN (Internet) default gateway the router communicates with.
DHCP Server	The IP address of the DHCP server which provided the IP configuration addresses.
DNS Server	The IP address of the DNS server which provides network name to IP address translation.
Lease Obtained	When the DHCP lease was obtained.
Lease Expires	When the DHCP lease was expires.
Release	Click the Release button to release the DHCP lease.
Renew	Click the Renew button to renew the DHCP lease.

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

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	1235017	2927810	0	723	2220	7 days 01:33:24
LAN1	100M/Full						1 day 01:06:26
LAN2	Link Down	220142	190203	0	1703	480	--
LAN3	Link Down						--
LAN4	Link Down						--
WLAN	11M/54M	164790	128056	0	160	41	7 days 01:33:28

Poll Interval: (secs)

Figure 4-3

This screen shows the following statistics:

Table 4-3: Router Statistics Items

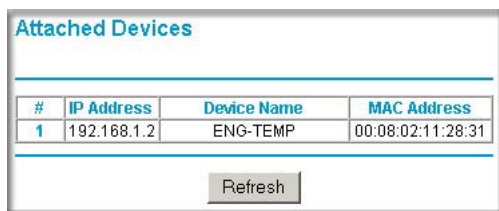
Item	Description
Port	The statistics for the WAN (Internet), the four LAN (local) and the WLAN (wireless Internet). For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.
Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.
Up Time	The amount of time since the router was last restarted.

Table 4-3: Router Statistics Items (continued)

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

Viewing a List of Attached Devices

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



#	IP Address	Device Name	MAC Address
1	192.168.1.2	ENG-TEMP	00:08:02:11:28:31

Figure 4-4

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

Configuration File Management

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

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

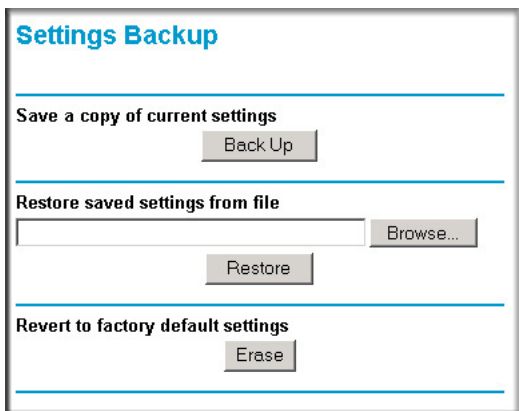


Figure 4-5

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

Restoring and Backing Up the Configuration

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

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

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



Warning: Do not interrupt the reboot process.

Erasing the Configuration

It is sometimes desirable to restore the router to original default settings. This can be done by using the Erase function, which will restore all factory settings. After an erase, the router's password will be **password**, the LAN IP address will be 192.168.1.1, and the router's DHCP client will be enabled.

To erase the configuration, click the Erase button.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See [“Restoring the Default Configuration and Password”](#) on page 6-7.

Upgrading the Router Software

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



Note: Before upgrading the router software, use the router backup utility to save your configuration settings. Any router upgrade will revert the router settings back to the factory defaults. After completing the upgrade, you can restore your settings from the backup.



Note: The Web browser used to upload new firmware into the Wireless Router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 and above and Netscape Navigator 4.7 and above.

To check for new firmware:

1. From the Main Menu of the browser interface, under the Maintenance heading, select Router Upgrade. The Router Upgrade screen will display.
2. Click Check to check for new firmware. If new firmware is available you will be directed to the appropriate new firmware upgrade location on the NETGEAR customer support website.
3. Select the new firmware version and save it to a location on your hard disk (usually the Temp folder).

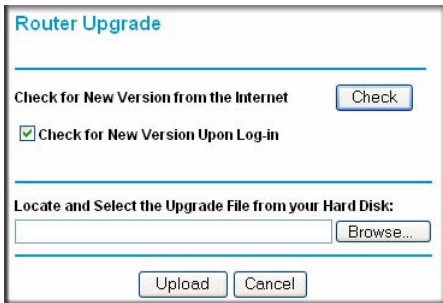



Figure 4-6

To upload new firmware:

1. In the Router Upgrade menu, click **Browse** and browse to the location where you saved the new version of the firmware.
2. Unzip (if the downloaded file is a .zip file) the new firmware file.
3. Click **Upload**.

	<p>Note: When uploading software to the Wireless Router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your router will automatically restart. The upgrade process will typically take about one minute.</p>
---	--

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

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.



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

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

Change Password

Old password

New password

Repeat new password

Figure 4-7

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

Chapter 5

Advanced Router Configuration

This chapter describes how to configure the advanced features of your Router Model WGR614v8. These features can be found under the Advanced heading in the Main Menu of the browser interface.



Note: If you are unfamiliar with networking and routing, refer to [Appendix B, “Related Documents,”](#) to become more familiar with the terms and procedures used in this chapter.

Setting up a Vista WPS Network

If you have configured your router from a Windows Vista PC using Wi-Fi Protected Setup (WPS) or if you configured your router using the NETGEAR wizard and selected one of the following as your security choice: no security, WPA, WPA2 or WPA+WPA2, then you can expand your network map and add additional clients by using the following features:

- **Allow a Registrar to Configure This Router.** When this is enabled, a Windows Vista PC can configure the router using WPS by adding the router’s PIN which is located on the router label. This is the default configuration until the router has been configured. Once a Windows Vista PC has configured the router, this feature becomes inactive. To reconfigure the router using a Windows Vista PC, this option must be enabled.
- **Enable Built-In Registrar.** When enabled, the router becomes the registrar and can easily add additional wireless clients into your network by automatically assigning the router’s Wireless Network Name (SSID) and WPA/WPA2-PSK security to the client. The client is added by entering the client PIN (which is promoted from the client utility) in the Add a Wireless Client dialog field.



Note: When using the Vista settings, all devices in your network must use the same security settings and Wireless Network Name (SSID) in order to interoperate with each other.

To configure the router from a Windows Vista PC:

1. If there is no check mark in the **Allow a Registrar to Configure this Router** checkbox, check the radio box and click Apply.
2. On the Windows Vista PC, click the Network icon on your desktop to view a dialog that displays your network devices.
3. From the Network dialog box, click the Add a wireless device menu button and follow the instructions displayed by the Windows Vista registrar.

Once a Windows Vista PC has configured the router, the **Allow a Registrar to Configure this Router** feature becomes inactive.

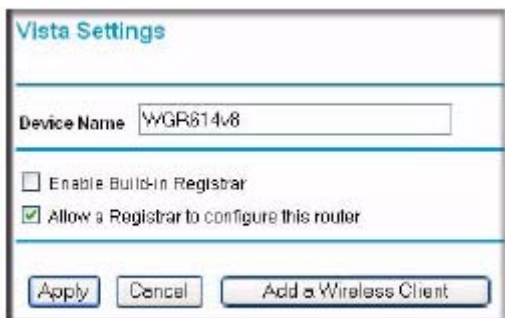



Figure 5-1

	<p>Note: The device name should be set to a name that is easy to identify in your network. You can see this name in the Vista network map and network explorer.</p>
---	--

To add a WPS client using the built-in registrar:

1. Select Vista Settings under the Advanced section of the main menu. The Vista Settings screen will display.
2. Select the **Enable Built-in Registrar** checkbox and click Apply. The Enable Built-in Registrar will be enabled.
3. Click Add a Wireless Client. The dialog box will prompt you for the client's PIN which is prompted from the client utility. (You should be able to view the client's PIN using the client's configuration utility.)
4. Click Add. The Wireless Client will be added to your network

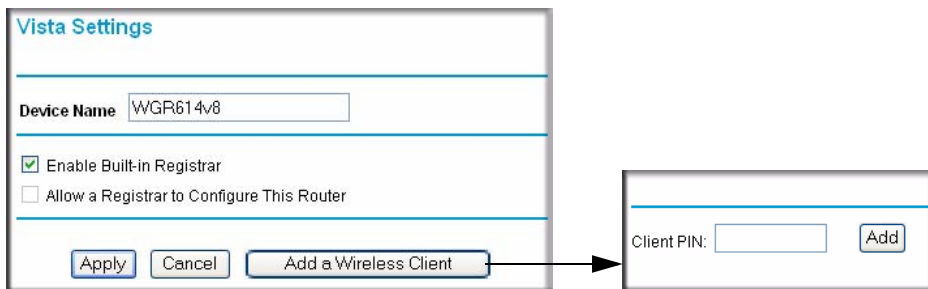


Figure 5-2

Configuring Port Triggering

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



Note: If you use applications such as multi-player gaming, peer-to-peer connections, real time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable UPnP according to the instructions at [“Using Universal Plug and Play \(UPnP\)”](#) on page 5-20.

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

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

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

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

Port Forwarding / Port Triggering

Please select the service type

Port Forwarding

Port Triggering

Disable Port Triggering

Port Triggering Timeout (in minutes)

Port Triggering Portmap Table

	#	Enable	Service Name	Service Type	Inbound Connection	Service User
<input type="radio"/>	1	<input checked="" type="checkbox"/>	dialpad_1	TCP:51200	TCP/UDP:51200	ANY
<input type="radio"/>	2	<input checked="" type="checkbox"/>	dialpad_2	TCP:51201	TCP/UDP:51201	ANY
<input type="radio"/>	3	<input checked="" type="checkbox"/>	paltalk_1	TCP:2090	TCP/UDP:2090	ANY
<input type="radio"/>	4	<input checked="" type="checkbox"/>	paltalk_2	TCP:2091	TCP/UDP:2091	ANY
<input type="radio"/>	5	<input checked="" type="checkbox"/>	quicktime	TCP:554	TCP/UDP:6970..6990	ANY
<input type="radio"/>	6	<input checked="" type="checkbox"/>	starcraft	TCP:6112	TCP/UDP:6112	ANY

Figure 5-3



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

- **Port Triggering Timeout**

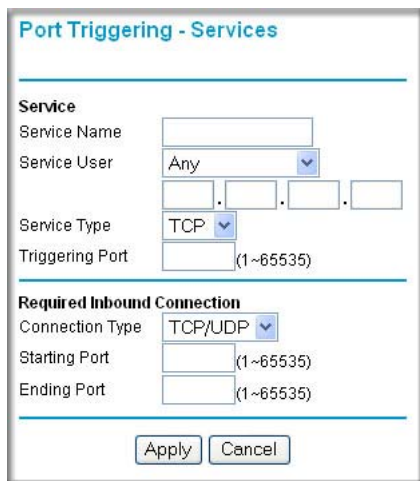
Enter a value up to 9999 minutes. The Port Triggering Timeout value controls the inactivity timer for the designated inbound port(s). The inbound port(s) will be closed when the inactivity timer expires.

- **For Internet Games or Applications**

Before starting, you'll need to know which service, application or game you'll be configuring. Also, you'll need to have the outbound port (triggering port) address for this game or application.

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

1. Click **Add**.



The screenshot shows a configuration window titled "Port Triggering - Services". It is divided into two main sections: "Service" and "Required Inbound Connection".

Service Section:

- Service Name: A text input field.
- Service User: A dropdown menu with "Any" selected.
- IP Address: A field with four sub-inputs separated by dots (IP address format).
- Service Type: A dropdown menu with "TCP" selected.
- Triggering Port: A text input field with "(1~65535)" as a hint.

Required Inbound Connection Section:

- Connection Type: A dropdown menu with "TCP/UDP" selected.
- Starting Port: A text input field with "(1~65535)" as a hint.
- Ending Port: A text input field with "(1~65535)" as a hint.

At the bottom of the window are two buttons: "Apply" and "Cancel".

Figure 5-4

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

Configuring Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make a local server (for example, a Web server or game server) visible and available to the Internet. This is done using the Port Forwarding menu. From the Main Menu of the browser interface, under Advanced, click on Port Forwarding to view the port forwarding menu, shown below.

Figure 5-5

Use the Port Forwarding menu to configure the router to forward incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a Default DMZ Server to which all other incoming protocols are forwarded. The DMZ Server is configured in the WAN Setup menu as discussed in [“Configuring the WAN Setup Options” on page 5-9](#).

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



Note: To assure that the same computer always has the same IP address, use the reserved IP address feature of your Wireless Router. See [“Using Address Reservation” on page 5-13](#) for instructions on how to use reserved IP addresses

To configure port forwarding to a local server:

1. From the Service & Game box, select the service or game that you will host on your network. If the service does not appear in the list, refer to the following section, ““[Adding a Custom Service](#)” on page 5-7”.
2. Enter the IP address of the local server in the corresponding Server IP Address box.
3. Click the Add button.

Adding a Custom Service

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

1. On the Port Forwarding/Port Triggering screen, click Add Custom Service.

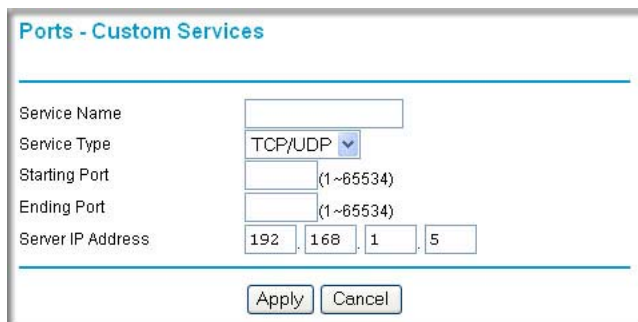


Figure 5-6

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

Editing or Deleting a Port Forwarding Entry

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

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

Local Web and FTP Server Example

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

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

Some considerations for this application are:

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

Multiple Computers for Half Life, KALI or Quake III Example

To set up an additional computer to play Half Life, KALI or Quake III:

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

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

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

Configuring the WAN Setup Options

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

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 5-7

Disabling the SPI Firewall

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

Setting Up a Default DMZ Server

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



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

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

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

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

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

Responding to Ping on Internet WAN Port

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

Setting the MTU Size

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

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

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

NAT Filtering

This option determines how the router deals with inbound traffic.

- The Secured option provides a secure firewall that protects the PCs on LAN from attacks coming from the Internet. However, some applications such as Internet games, point-to-point applications, or multimedia applications may not function properly
- The Open option provides a much less secure firewall, but it does allow almost all Internet applications to function.

Using the LAN IP Setup Options

The second feature category under the Advanced heading is LAN IP Setup. This menu allows configuration of LAN IP services such as DHCP and RIP. From the Main Menu of the browser interface, under Advanced, click on LAN IP Setup to view the LAN IP Setup menu, shown below.

LAN IP Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 1 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: Disabled

Use Router as DHCP Server

Starting IP Address: 192 . 168 . 1 . 2

Ending IP Address: 192 . 168 . 1 . 51

Address Reservation

#	IP Address	Device Name	Mac Address
---	------------	-------------	-------------

Add Edit Delete

Apply Cancel

Figure 5-8

Configuring LAN TCP/IP Setup Parameters

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

- LAN IP addresses – 192.168.1.1
- Subnet mask – 255.255.255.0

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

The LAN IP parameters are:

- **IP Address:** This is the LAN IP address of the router.
- **IP Subnet Mask:** This is the LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
- **RIP Direction:** RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. None is the default.
 - When set to Both or Out Only, the router will broadcast its routing table periodically.
 - When set to Both or In Only, it will incorporate the RIP information that it receives.
 - When set to None (default), it will not send any RIP packets and will ignore any RIP packets received.
- **RIP Version:** This controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.
 - RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
 - RIP-2 carries more information. RIP-2B uses subnet broadcasting.



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

Using the Router as a DHCP server

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

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory (see [Appendix B, "Related Documents"](#) for an explanation of DHCP and information about how to assign IP addresses for your network).

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

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 and 192.168.1.253, although you may wish to save part of the range for devices with fixed addresses.

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

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the router's LAN IP address)
- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router's LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu)

Using Address Reservation

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

To reserve an IP address:

1. On the LAN IP Setup Screen, click Add. The Address Reservation screen will display.

Address Reservation

Address Reservation Table

#	IP Address	Device Name	MAC Address
1	192.168.1.2	--	00:08:02:11:28:31

IP Address . . .

MAC Address

Device Name

Figure 5-9

2. In the IP Address box, type the IP address to assign to the computer or server. (choose an IP address from the router's LAN subnet, such as 192.168.1.X)
3. Type the MAC Address of the computer or server. (Tip: If the computer is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.)
4. Click Apply to enter the reserved address into the table.



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

To edit or delete a reserved address entry:

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

Using a Dynamic DNS Service

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

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



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

The router contains a client that can connect to many popular dynamic DNS services. You can select one of these services and obtain an account with them. Then, whenever your ISP-assigned IP address changes, your router will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

From the Main Menu of the browser interface, under Advanced, click on Dynamic DNS.

Dynamic DNS

Use a Dynamic DNS Service

Service Provider:

Host Name:

User Name:

Password:

Use Wildcards

Apply Cancel Show Status

Figure 5-10

To configure Dynamic DNS:

1. Register for an account with one of the dynamic DNS service providers whose names appear in the 'Select Service Provider' box. For example, for dyndns.org, go to www.dyndns.org.
2. Select the Use a dynamic DNS service check box.
3. Select the name of your dynamic DNS Service Provider.
4. Type the Host Name (or domain name) that your dynamic DNS service provider gave you.
5. Type the User Name for your dynamic DNS account.
6. Type the Password (or key) for your dynamic DNS account.

- If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Use wildcards check box to activate this feature.
For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
- Click Apply to save your configuration.

Configuring Static Routes

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

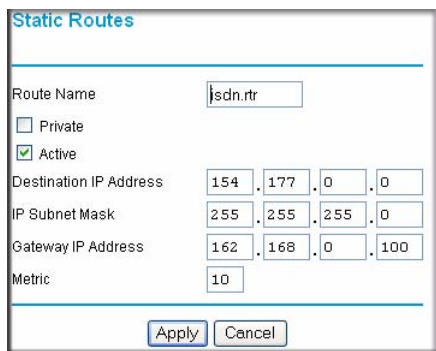
From the Main Menu of the browser interface, under Advanced, select Static Routes. The Static Route will display.



Figure 5-11

To add or edit a Static Route:

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

The screenshot shows the "Add/Edit" menu for a static route. It includes the following fields and options:

- Route Name:
- Private
- Active
- Destination IP Address: . . .
- IP Subnet Mask: . . .
- Gateway IP Address: . . .
- Metric:

At the bottom are "Apply" and "Cancel" buttons.

Figure 5-12

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



#	Active	Name	Destination	Gateway
1	Yes	isdn.rtr	154.177.0.0	162.168.0.100

Buttons: Add, Edit, Delete

Figure 5-13

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 is 134.177.0.0.

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

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

In this example:

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

Enabling Remote Management Access

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



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

Remote Management

Turn Remote Management On

Remote Management Address:
10.1.1.156:8080

Allow Remote Access By:

Only This Computer: . . .

IP Address Range: From . . .
To . . .

Everyone

Port Number:

Figure 5-14

To configure your router for Remote Management:

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



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

3. To specify the type of Internet access:
 - a. Select Everyone to allow access from any IP address on the Internet.
 - b. Select IP address range to allow access from a range of IP addresses on the Internet. Enter a beginning and ending IP address to define the allowed range.
 - c. Select Only this computer to allow access from a single IP address on the Internet. Enter the IP address that will be allowed access.

4. Specify the Port Number that will be used for accessing the management interface.

Web browser access normally uses the standard HTTP service port 80. For greater security, change the remote management Web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click Apply to have your changes take effect.



Note: When accessing your router from the Internet, you will type your router's WAN IP address into your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, you must enter `http://134.177.0.123:8080` in your browser. The Remote Management Address from the Remote Management Window (see [Figure 5-14](#)) is the address you will enter in your browser's address field.

Using Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

UPnP

Turn UPnP On

Advertisement Period (in minutes)

Advertisement Time To Live (in hops)

UPnP Portmap Table

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

Figure 5-15

From the Main Menu of the browser interface, under Advanced, click on UPnP. Set up UPnP according to the guidelines below.

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



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

- **Advertisement Period:** The Advertisement Period is how often the router will broadcast its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.

- **Advertisement Time To Live:** The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.
- **UPnP Portmap Table:** The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.


Chapter 6

Troubleshooting

This chapter gives information about troubleshooting your Router Model WGR614v8. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

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

1. When power is first applied, verify that the Power light  is on.
2. After approximately 10 seconds, verify that:
 - a. The power light is solid green.
 - b. The LAN port lights are lit for any local ports that are connected.
 - c. The Internet port light is lit.

If a port's light is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's light is green. If the port is 10 Mbps, the light will be amber.

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

Power Light Not On

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

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC 1A power adapter supplied by NETGEAR for this product.

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

Lights Never Turn Off

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

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

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.1.1. This procedure is explained in [“Restoring the Default Configuration and Password” on page 6-7](#).

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

LAN or WAN Port Lights Not On

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

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

When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the router's Web Configuration interface from a computer on your local network, check the following:

- Check the Ethernet connection between the computer and the router as described in the previous section.

- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254. Refer to "Internet Networking and TCP/IP Addressing" to find your computer's IP address, and follow the instructions in "Preparing Your Network for Internet Access" to configure your computer in [Appendix B](#), "Related Documents."



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

- If your router's IP address has been changed and you don't know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.1.1. This procedure is explained in "[Restoring the Default Configuration and Password](#)" on page 6-7.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

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

Troubleshooting the ISP Connection

If your router is unable to access the Internet, you should first determine whether the router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

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

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

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

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

- Your ISP may require a login program.
Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP may check for your computer's host name.
Assign the computer Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:

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

OR

Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu.

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

- Your computer may not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address. Alternatively, you may configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer may not have the router configured as its TCP/IP gateway.

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

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer or workstation.

Testing the LAN Path to Your Router

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

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

1. From the Windows toolbar, click on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the router, as in this example:
`ping 192.168.1.1 (or routerlogin.net)`
3. Click on OK.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
 - Make sure the LAN port LED is on. If the LED is off, follow the instructions in “[LAN or WAN Port Lights Not On](#)” on [page 6-2](#).
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
 - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where *<IP address>* is the IP address of a remote device such as your ISP’s DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information will not be visible in your computer’s Network Control Panel. Verify that the IP address of the router is listed as the default gateway.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
 - If your ISP assigned a host name to your computer, enter that host name as the Account Name in the Basic Settings menu.
 - Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to “clone” or “spoof” the MAC address from the authorized computer.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to 192.168.1.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the router (see [“Erasing the Configuration” on page 4-7](#)).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the router.

1. Press and hold the Default Reset button until the power light blinks on (about 10 seconds).
2. Release the Default Reset button and wait for the router to reboot.

If the wireless router fails to restart or the power light continues to blink or turns solid amber, the unit may be defective. If the error persists, you might have a hardware problem and should contact technical support.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The Wireless Router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The router does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked “Adjust for Daylight Savings Time”.

Appendix A

Technical Specifications

This appendix provides technical specifications for the Router Model WGR614v8.

Specification	Description
Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)
Power Adapter	
North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1A output, 12W maximum
Physical Specifications	
Dimensions:	28 x 175 x 119 mm (1.1 x 6.89 x 4.68 in.)
Weight:	0.26 kg (0.57 lb)
Environmental Specifications	
Operating temperature:	0° to 40° C (32° to 104° F)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B EN301489, EN300328, EN60950 C-Tick
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T or 100BASE-Tx, RJ-45

Specification	Description
Wireless	
Radio Data Rates	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps Auto Rate Sensing
Frequency	2.4-2.5Ghz
Data Encoding:	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes.
Operating Frequency Ranges:	2.412~2.462 GHz (US) 2.412~2.472 GHz (Japan) 2.412~2.472 GHz (Europe ETSI)
802.11 Security:	40-bits (also called 64-bits) and 128-bits WEP; and WPA-PSK, WPA2-PSK and WPA-PSK+WPA2-PSK
Default Factory Settings	
Wireless Access Point	Enabled
Wireless Access List (MAC Filtering)	All wireless stations allowed
SSID broadcast	Enabled
SSID	NETGEAR
11b/g RF Channel	11
Mode	g and b
Authentication Type	Open System
Security	Disabled
Allow a Registrar to configure this router	Enabled

Appendix B

Related Documents

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

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

