108 Mbps Wireless Router WGT624 v4 Reference Manual

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

202-10234-01
May 2007

Trademarks

NETGEAR is a trademark of Netgear, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

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

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

Maximum Wireless Signal Rate Derived from IEEE Standard 802.11 Specifications

Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

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

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

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

The device and its antenna(s) must not be co-located or operating in conjuncyion with any other antenna or trasmitter.
For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.

FCC Radiation Exposure Statement：

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

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies 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 undersired operation.

EN 55 022 Declaration of Conformance

This is to certify that the WGT624 v4 108 Mbps Wireless Router is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das WGT624 v4 108 Mbps Wireless Router 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.

Hereby, NETGEAR, declares that this device is in compliance with the essential requirements and other relevant provisions of R&TTE Directive 1999/5/EC. This device will be sold in the following EEA countries：Austria, Italy, Belgium, Liechtenstein, Denmark, Luxembourg, Finland, Netherlands, France, Norway, Germany, Portugal, Greece, Spain, Iceland, Sweden, Ireland, United Kingdom, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Malta, Slovakia, Poland. Slovenia.

It is hereby certified that the WGT624 v4 108 Mbps Wireless Router 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 see the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your WGT624 v4 108 Mbps Wireless Router.

World Wide Web

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

Product and Publication Details

Model Number:	WGT624 v4
Publication Date:	May 2007
Product Family:	Wireless Router
Product Name:	WGT624 v4 108 Mbps Wireless Router
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10234-01

Contents

108 Mbps Wireless Router WGT624 v4 Reference Manual

About This Manual

Chapter 1
Connecting the Router to the Internet

Chapter 2
Wireless Settings and Security

Chapter 3
Content Filtering

Chapter 4
Maintenance

Chapter 5
Advanced Configuration

Chapter 6
Troubleshooting

Appendix A
Technical Specifications and Default Configuration

About This Manual

The *NETGEAR® 108 Mbps Wireless Router WGT624 v4 Reference Manual* describes how to install, configure, and troubleshoot the WGT624 v4 108 Mbps Wireless Router. 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:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed`	Screen text and commands,

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

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

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

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

- **Scope.** This manual is written for the WGT624 v4 wireless router according to these specifications:

Product version	WGT624 v4 108 Mbps Wireless Router
Manual publication date	May 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. website at *http://www.netgear.com/support*.

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print This Manual

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

- **Printing a page in the HTML view**.

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

- **Printing a chapter**.

  Use the PDF of This Chapter link at the top left of any page.

  – Click the PDF of This Chapter link at the top 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.

  – 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 website at *http://www.adobe.com*.

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

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

- **Printing the full manual**.

  Use the Complete PDF Manual link at the top left of any page.

  - Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
  - Click the print icon in the upper left of the window.

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

Chapter 1
Connecting the Router to the Internet

The WGT624 v4 108 Mbps 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. For information about product features and compatible NETGEAR products, see the NETGEAR website at *http://www.netgear.com*.

This chapter describes how to connect your router and how to access the Internet through it.

After the router is connected to the Internet and your wireless connections are working, you should implement wireless security (Chapter 2, "Wireless Settings and Security". You can also configure content filtering (Chapter 3, "Content Filtering), and advanced users can configure maintenance (Chapter 4, "Maintenance) and advanced settings (Chapter 5, "Advanced Configuration").

What Is in the Box

The product package should contain the following items:

- The wireless router
- An AC power adapter (varies by region)
- Vertical stand
- A yellow Ethernet cable
- *108 Mbps Wireless Router WGRT624 v4 Resource CD*, including:
  - The Smart Wizard Installation Assistant
  - This manual
- Warranty and Support Information cards

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 product for repair.

Wireless Router

Take a moment to become familiar with the router. The following sections describe the bottom label, front view, and back view.

Bottom Label

View the label on the bottom of the wireless router to identify the serial number, security PIN number, port connectors, status lights, and default login information.

Status Lights on the Front

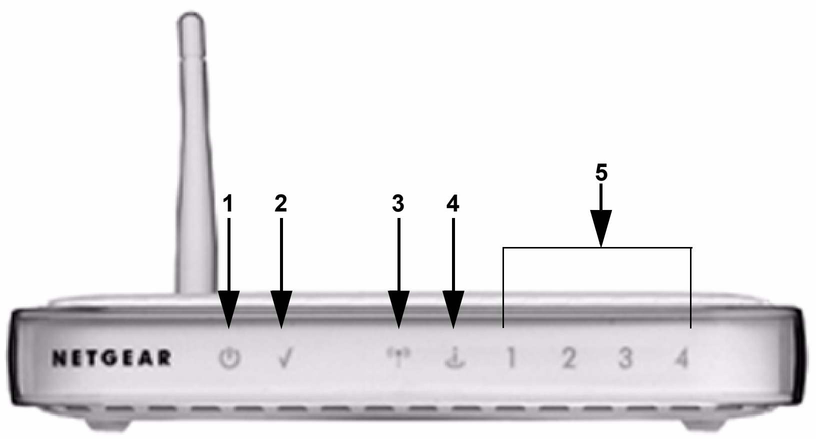


Figure 1-1

You can use the status lights on the front of the wireless router to verify various conditions.

Table 1-1. Status Lights

Status Light	Activity	Description
1. Power	On Off	Power is supplied to the router. Power is not supplied to the router.
2. Test	On Blink Off	The system is initializing or the Reset button was pressed in for 5 seconds. Firmware upgrade in process, or factory default settings have been restored. The system is ready and running.

Table 1-1. Status Lights (continued)

3. Wireless	On Blink Off	Indicates that the Wireless radio is enabled. Data is being transferred. The wireless router radio is off. (See "Advanced Wireless Settings" in Chapter 2.)
4. Internet	On (Amber) On (Green) Blink (Green) Off	The Ethernet cable is connected, but the wireless router has not received an Internet address. The wireless router has an Internet address. Data is being communicated with the Internet. No link is detected on this port.
5. LAN (Local Area Network) Lights 1–4	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The local port is connected to a 100 Mbps device. Data is being transmitted at 100 Mbps. The local port has detected a link with a 10 Mbps device. Data is being transmitted at 10 Mbps. No link is detected on this port.

Port Connections on the Back

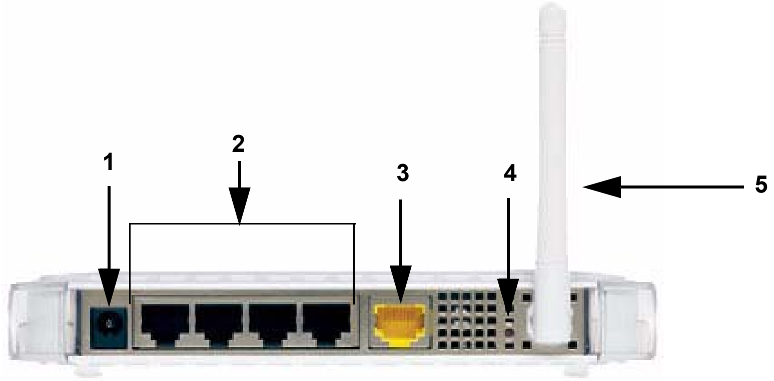


Figure 1-2

The back of the wireless router has the following port connections:

1. Power adapter port
2. Four local Ethernet (LAN) 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

Preparing to Set Up Your Wireless Router

Prepare the following before you set up your router:

- Internet service.
- The configuration information your Internet service provider (ISP) gave you. Depending on how your Internet account was set up, your may need one or more of these settings for the wireless router to access the Internet:
  - Host and domain names
  - Internet login name and password (frequently an e-mail address and password)
  - Domain name server (DNS) Addresses
  - Fixed or static IP address

  Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it.
- For cable modem service, use the computer you first used to set up your Internet service.
- For suggestions about the best location to place your router, see "Optimizing Your Wireless Connections" on page 2-1.

Two Setup Methods: 1) Smart Wizard Setup 2) Manual Setup

You have two methods available for setting up your wireless router.

- **Smart Wizard setup**: Click Setup on the CD to use the Smart Wizard.
  - This option is the easiest. The wizard guides you through the setup process, automates many of the steps, and verifies that necessary conditions exist and that steps you perform have been successfully completed.
  - This option requires a PC running Microsoft Windows.
- **Manual setup**: This option is best if you cannot use the wizard on the CD, are replacing an existing wireless router, or are technically knowledgeable. Follow the instructions in this manual to set up your wireless router.

Use the setup option that best suits you.

Smart Wizard Installation

Note: Do not change your existing Internet connection. Instead, let the Smart Wizard Installation Assistant on the *108 Mbps Wireless Router WGRT624 v4 Resource CD* guide you through the setup process.

The wizard setup process should take about 20 minutes to complete. Follow these step:

1. Insert the NETGEAR *108 Mbps Wireless Router WGRT624 v4 Resource CD* into a Windows PC with an Internet connection. The Welcome screen appears:

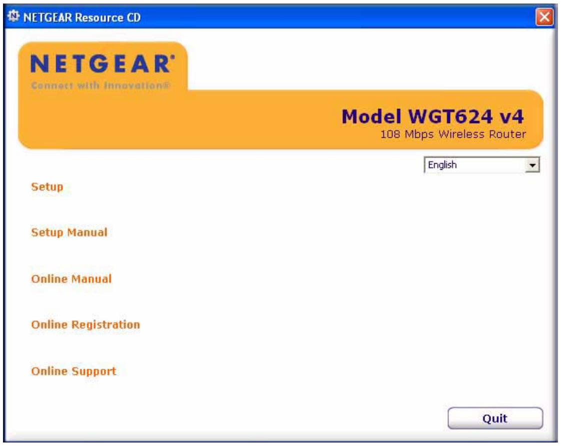
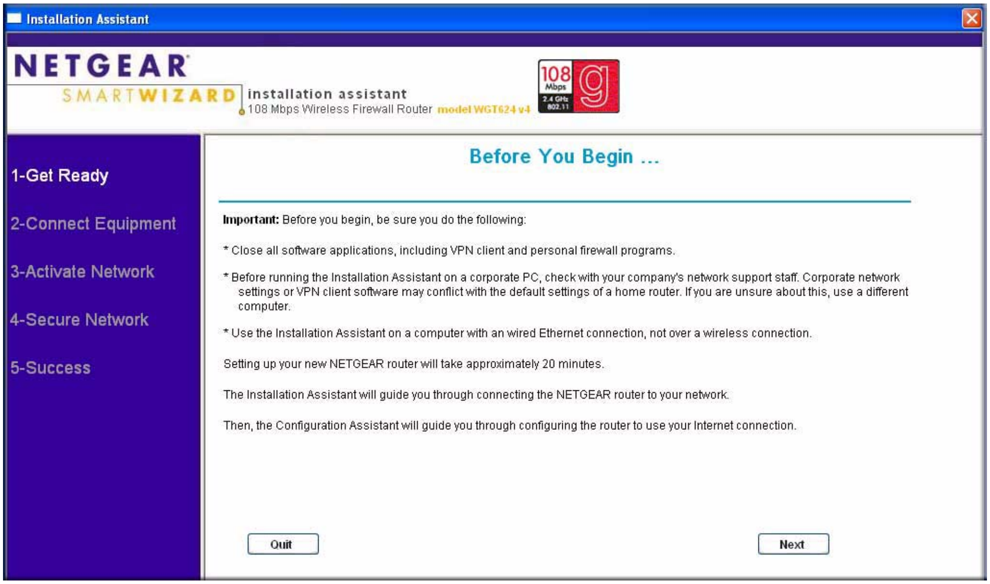


Figure 1-3

The CD detects the language you are using on your PC. Accept the language, or change to a different language.

Note: If the CD does not automatically start, browse the CD, and then double-click Autorun.

2. Click Setup. The Smart Wizard Installation Assistant opens:



Before You Begin ...

Important: Before you begin, be sure you do the following:

* Close all software applications, including VPN client and personal firewall programs.

* Before running the Installation Assistant on a corporate PC, check with your company's network support staff. Corporate network settings or VPN client software may conflict with the default settings of a home router. If you are unsure about this, use a different computer.

* Use the Installation Assistant on a computer with an wired Ethernet connection, not over a wireless connection.

Setting up your new NETGEAR router will take approximately 20 minutes.

The Installation Assistant will guide you through connecting the NETGEAR router to your network.

Then, the Configuration Assistant will guide you through configuring the router to use your Internet connection.

Figure 1-4

3. Follow the wizard instructions.The Smart Wizard Installation Assistant will guide you through the setup process to:
   - Connect equipment: Follow onscreen instructions to connect your router.
   - Activate your network: The wizard detects your Internet connection and network name. The network name is the service set identifier (SSID).
   - Secure your network with wireless security: You can set up wireless security now, or choose to set it up later. NETGEAR strongly recommends using security. See Chapter 2, "Wireless Settings and Security".

4. A Success page opens after you have connected to the Internet and entered your wireless settings.

Manual Setup

There are two steps to setting up your wireless router:

1. Connect the router to the ADSL or cable modem, and connect a computer to the router.

➡	**Note:** Your computer has to be set to automatically get its TCP/IP network settings from the router via DHCP. This is usually the case. If you are unsure about this, use the wizard on the CD, which automatically takes care of this for you, or refer to the documentation for your computer.

2. Configure the router to use your Internet service.

Connecting Your Wireless Router

To connect your wireless router:

1. Connect the wireless router, the computer, and the modem.
   a. Turn off your computer.
   b. Turn off and unplug the cable or ADSL broadband modem.
   c. Locate the Ethernet cable (**1**) that connects your computer to the modem.

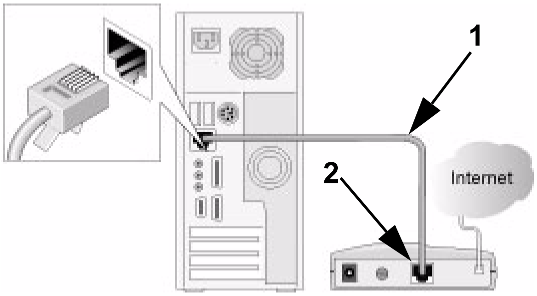


Figure 1-5

   d. Disconnect the cable at the modem end only (**2**).

e. Securely insert the free end of the cable (**1**) into a LAN port on the router, such as LAN port 4 (**3**).

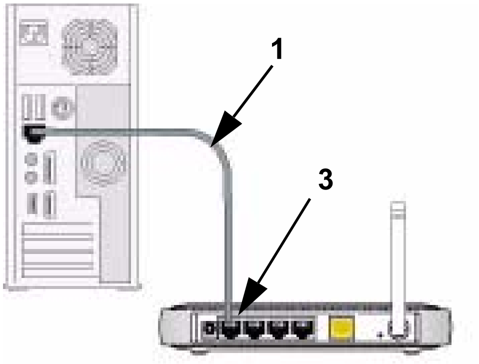


Figure 1-6

f. Securely insert the yellow cable (**5**) that came with your wireless router into the yellow Internet port of the wireless router (**4**) and the other end into the modem (**2**).

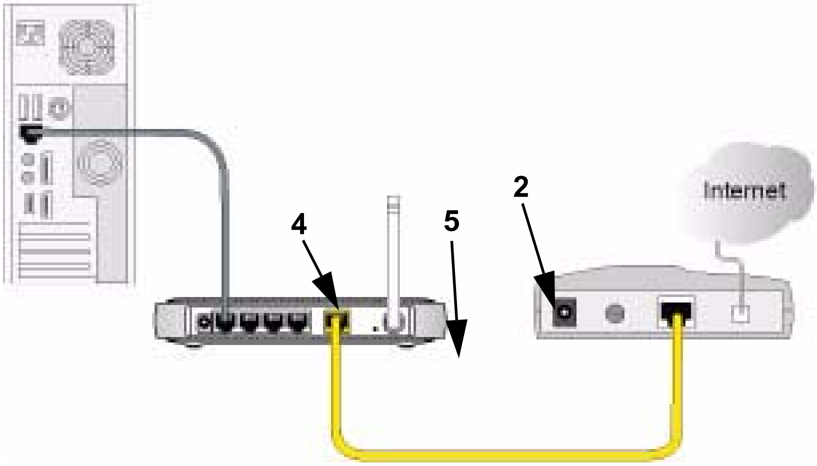


Figure 1-7

Your network cables are connected, and you are ready to start your network.

2. Start your network in the correct sequence.

⚠	**Warning:** Failure to start or restart your network in the correct sequence could prevent you from accessing the Internet.

a. First, plug in and turn on the cable or DSL modem. Wait 2 minutes.

b. Now, plug the power cord into your wireless router and into a power outlet. Wait 1 minute.

c. Last, turn on your computer.

➡	**Note:** For DSL customers, if software logs you in to the Internet, *do not* run that software. You may need to go to the Internet Explorer Tools menu > Internet Options > Connections tab page and select “Never dial a connection.”

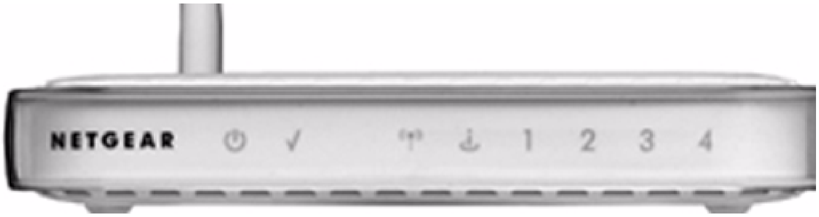


Figure 1-8

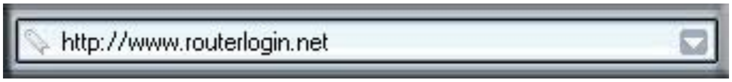
d. Check the wireless router status lights to verify the following:

- ⏻ **Power:** The power light should turn solid blue. If it does not, see “Power LED Not On” in Chapter 6.
- ✓ **Test:** The test light should turn solid green when the router is first turned on, then go off. If after 2 minutes it is still on, see “Basic Functioning” in Chapter 6.
- **Wireless:** The wireless light should be on. The Smart Wizard sets up the wireless feature of your router.
- **Internet:** The Internet port light should be lit. If it is not, make sure that the Ethernet cable is securely attached to the wireless router Internet port and that the modem, and the modem is powered on.
- 1 **LAN:** A LAN light should be lit. Green indicates that your computer is communicating at 100 Mbps; amber indicates 10 Mbps. If a LAN light is not lit, check that the Ethernet cable from the computer to the router is securely attached at both ends, and that the computer is turned on.

Setting Up Your Router for Internet Access

To access the router using its login name and password, follow these instructions.

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



http://www.routerlogin.net

Figure 1-9

Tip: You can connect to the wireless router by typing any one of these three URLs in the address field of your browser, then clicking Enter:

http://www.routerlogin.net

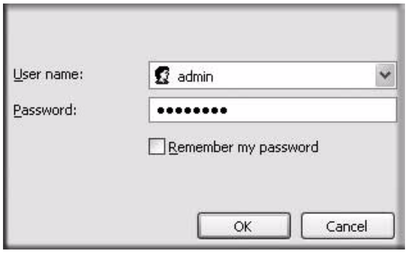
http://www.routerlogin.com

http://192.168.1.1

2. For security reasons, the router has its own user name and password. When prompted, enter **admin** for the user name and **password** for the router password, both in lowercase letters.

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

A login window opens.



User name: admin

Password: ••••••••

☐ Remember my password

Figure 1-10

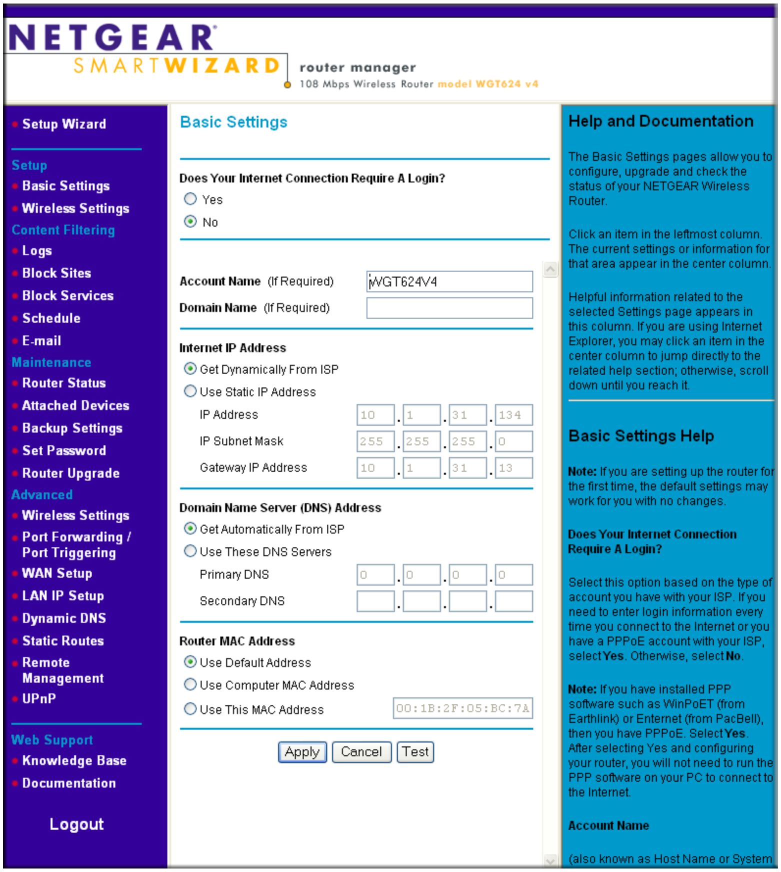
3. Click OK. The Firmware Upgrade Assistant opens.

4. Click Yes to check for new firmware in the NETGEAR database. (If you select No, you can check for new firmware later; see "Upgrading the Router Firmware" on page 4-3.)

   If new firmware is available, follow the onscreen instructions on the NETGEAR website to upgrade the firmware.

➡	**Note:** Usually the firmware image is an .img (or .chk) file and does not need to be decompressed before you can use it. If, however, the file is a .zip file, then the image is compressed and must be "unzipped" before you can use the file. On Windows computers, you can use WinZip utility to unzip the file.

When you have entered a user name and password, your Web browser displays the wireless router's home page:



Basic Settings

Does Your Internet Connection Require A Login?

○ Yes
● No

Account Name (If Required): WGT624V4

Domain Name (If Required):

Internet IP Address

● Get Dynamically From ISP
○ Use Static IP Address

IP Address: 10 . 1 . 31 . 134

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 10 . 1 . 31 . 13

Domain Name Server (DNS) Address

● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: . . .

Router MAC Address

● Use Default Address
○ Use Computer MAC Address
○ Use This MAC Address: 00:1B:2F:05:BC:7A

Help and Documentation

The Basic Settings pages allow you to configure, upgrade and check the status of your NETGEAR Wireless Router.

Click an item in the leftmost column. The current settings or information for that area appear in the center column.

Helpful information related to the selected Settings page appears in this column. If you are using Internet Explorer, you may click an item in the center column to jump directly to the related help section; otherwise, scroll down until you reach it.

Basic Settings Help

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

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.

Account Name

(also known as Host Name or System

Figure 1-11

For more help with connecting to the Internet, see "Changing Your Internet Settings Manually" on page 1-13.

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

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

Resolving an Internet Connection Problem

You can change your Internet settings after they have been configured by the Smart Wizard. See "Changing Your Internet Settings" on page 1-12.

If you do not successfully connect to the Internet:

1. Go through the settings and make sure you selected the correct options and typed everything correctly.
2. Contact your ISP to verify the configuration information.
3. For help with troubleshooting see:
   - Chapter 6, "Troubleshooting"
   - Troubleshooting in the *Router Setup Manual* on the *108 Mbps Wireless Router WGRT624 v4 Resource CD*
4. Contact NETGEAR Technical Support.

Changing Your Internet Settings

You can use the Smart Setup Wizard to change your Internet settings, or you can change them manually.

Using the Smart Setup Wizard to Change Your Internet Settings

You can use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection. The Smart Setup Wizard is not the same as the Smart Wizard Installation Assistant that appears only when the router is in its factory default state. After you set up the wireless router, the Smart Wizard Installation Assistant will not appear again.

To use the Smart Setup Wizard:

1. Connect to the wireless router by typing **http://www.routerlogin.net** in the address field of your browser, then click Enter.
2. For security reasons, the router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lowercase letters. To change the password, see "Changing the Administrator Password" on page 4-6.

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

   Once you have entered your user name and password, your Web browser should find the WGT624 v4 wireless router and display the home page as shown in Figure 1-11 on page 1-11.
3. Click Setup Wizard on the upper left of the main menu.
4. Click Next to proceed. Input your ISP settings, as needed.
5. At the end of the Setup Wizard, click the Test button to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 6, "Troubleshooting".

Changing Your Internet Settings Manually

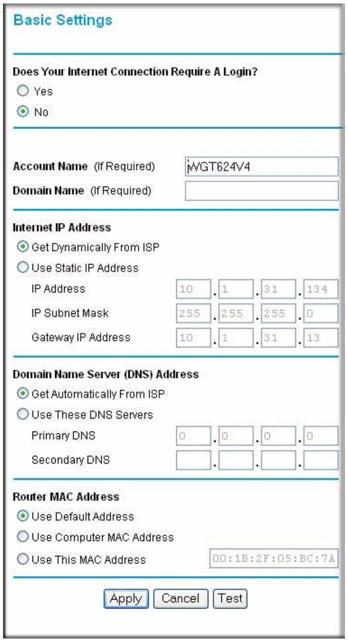
Note: If you are setting up the router for the first time, the default settings may work for you with no changes.

To change your Internet settings manually:

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

2. Click Basic Settings in the main menu. The basic settings depend on whether or not your Internet connection requires a login.

Basic Settings, No Login



Basic Settings

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

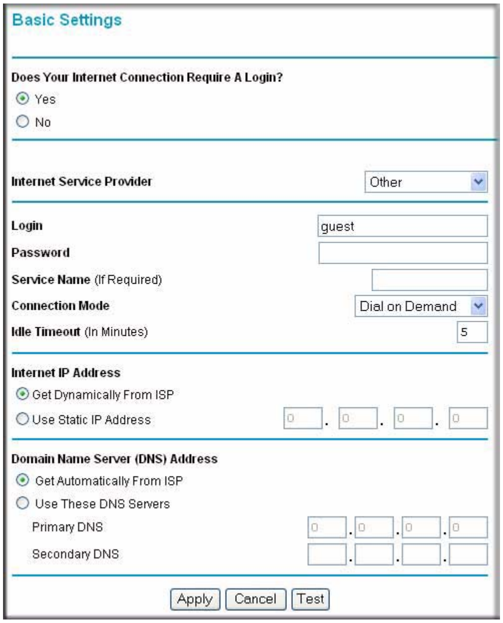
Account Name (If Required) WGT624V4
Domain Name (If Required)

Internet IP Address
● Get Dynamically From ISP
○ Use Static IP Address
IP Address 10 . 1 . 31 . 134
IP Subnet Mask 255 . 255 . 255 . 0
Gateway IP Address 10 . 1 . 31 . 13

Domain Name Server (DNS) Address
● Get Automatically From ISP
○ Use These DNS Servers
Primary DNS 0 . 0 . 0 . 0
Secondary DNS . . .

Router MAC Address
● Use Default Address
○ Use Computer MAC Address
○ Use This MAC Address 00:1B:2F:05:BC:7A

Basic Settings, Login Required



Basic Settings

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

Internet Service Provider Other

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

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

Domain Name Server (DNS) Address
● Get Automatically From ISP
○ Use These DNS Servers
Primary DNS 0 . 0 . 0 . 0
Secondary DNS . . .

Figure 1-12

3. Enter the settings for your Internet connection. These settings are explained in “Basic Settings for Your Internet Connection” on page 1-15.
   - Click an item in the column on the left. The current settings or information for that area appear in the center column.
   - Helpful information related to the selected Settings page appears in this column. If you are using Internet Explorer, you may click an item in the center column to jump directly to the related help section; otherwise, scroll down until you reach it.
4. Click **Test** to connect to the NETGEAR website. When you verify that you are connected, you can click **Logout** to exit.

For the most current documentation, go to: *http://www.netgear.com/support*.

Basic Settings for Your Internet Connection

The basic settings are explained below:

- **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 computer to connect to the Internet.

- **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.
  - **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 field.

    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.
  - **Password**: Type the password that you use to log in to your ISP.
  - **Service Name**: If your ISP provided a service name, enter it here. Otherwise, this may be left blank.
  - **Connection Mode:** Set the Connection Mode to Dial on Demand, Always, or Manually Connect.

    With the default setting, **Dial on Demand**, a PPPoE/PPTP/BigPond connection automatically starts when there is outbound traffic to the Internet, and it automatically terminates if the connection is idle based on the value in the Idle Timeout setting.

    When the Connection Mode is set to **Always On**, the PPPoE/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.

    If you select **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 it.

  - **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 reconnecting immediately whenever the connection is lost.

- **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 **Get dynamically from ISP**.

  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 then type in the IP address.

- **Account Name** (also known as host name or system name): For most users, type your account name or user name in this box. For example, if your main mail account is JerAB@ISP.com, then type JerAB here. If your ISP has given you a specific host name, then type it (for example, CCA7324-A).

- **Domain Name**: For most users, you may leave this box blank, unless required by your ISP. You may type the domain name of your ISP. For example, if your ISP's mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the Domain Name.

  If you have a domain name given to you by your ISP, type it in this box. (For example, Earthlink Cable may require a host name of "home" and Comcast sometimes supplies a domain name.)

  If you have a cable modem, this is usually the workgroup name.

- **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 **Get Dynamically From ISP**.

  If you have a fixed (or static IP) address, your ISP will have provided you with the required information. Select **Use Static IP Address** and type the IP address, subnet mask and gateway IP address.

  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.

If your ISP gave you one or two DNS addresses, select **Use These DNS Servers,** and then type the primary and secondary addresses. Otherwise, select **Get Automatically From ISP**.

➡	**Note:** If you get "Address not found" errors when you go to a website, it is likely that your DNS servers are not 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.

  Usually, select **Use Default MAC Address**.

If your ISP requires MAC authentication, then select either "Use Computer MAC address" to disguise the router's MAC address with the computer's own MAC address or "Use This MAC Address" to manually type 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.

Product Registration, Support, and Documentation

Register your product at *http://www.NETGEAR.com/register*. Registration is required before you can use our telephone support service. Product updates and Web support are always available by going to: *http://kbserver.netgear.com/*.

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

Chapter 2
Wireless Settings and Security

This chapter describes how to set up the wireless features of your WGT624 v4 wireless router. In planning your wireless network, select a location for the wireless router that will maximize performance. Also, consider the level of wireless security required.

➡	**Note:** The router factory default settings are shown in "Default Configuration Settings" in Appendix A. You can restore these defaults with the Reset button on the rear panel.

Optimizing Your Wireless Connections

The speed and range of your wireless connection can vary significantly based on the location of the wireless router. Choose a location for your router that will maximize the network speed.

To optimize wireless router performance:

- Identify critical wireless links.
  If your network has several wireless devices, decide which wireless devices need the highest data rate, and locate the router near them. Many wireless products have automatic data-rate fallback. This lets you connect from farther away, but the connection may also be slower. So the most critical wireless links are those where the traffic is high and the distances are great.
- Choose placement carefully.
  For best results, place your router:
  - Near the center of the area in which your computers will operate.
  - In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
- Avoid obstacles to wireless signals.
  - Keep wireless devices at least 2 feet from large metal fixtures such as file cabinets, refrigerators, pipes, metal ceilings, reinforced concrete, and metal partitions.
  - Keep the devices away from large amounts of water such as fish tanks and water coolers.

- Reduce interference.
  Avoid windows unless you want to communicate between buildings.
  Place wireless devices away from electromagnetic noise sources, especially those in the 2400–2500 MHz frequency band. Common noise-creating sources are:
  - Computers and fax machines (no closer than 1 foot)
  - Copying machines, elevators, and cell phones (no closer than 6 feet)
  - Microwave ovens (no closer than 10 feet)
- Choose your settings.
  - Use a scanning utility to determine which other wireless networks are operating nearby, and choose an unused channel.
  - Turn off SSID Broadcast, and change the default SSID. Other nearby devices may automatically try to connect to your network several times a second, which can cause significant performance reduction.

Setting Up Your Wireless Connections

> ➔ **Note:** Before you can set up your wireless connections, you must install the router and connect to the Internet. See Chapter 1, “Connecting the Router to the Internet”.

When you are setting up wireless connections, these guidelines will help make the process simpler and easier:

- Use an Ethernet cable to connect your computer to the router when you are setting up or changing wireless settings. If you are connected wirelessly and make a change, you will lose your wireless connection when you apply the change.
- Remember to note what your wireless settings are. For help keeping track of them, see “Information to Gather Before Changing the Wireless Settings” on page 2-3.
- Wait until after your wireless connection is up and running before you enable wireless security (“Understanding Wireless Security” on page 2-6).

Information to Gather Before Changing the Wireless Settings

Before changing your wireless settings, print this form and record the following information. For an existing wireless network, the person who set up or is responsible for the network can provide this information. After you set up wireless security for the router, you must set up each computer with the same wireless security settings in order to for it to join the wireless network.

- **Wireless network name (SSID)*:*** ______________________________ The SSID, also called the wireless network name, for the wireless network. You can use up to 32 alphanumeric characters. The SSID *is* case-sensitive.
- **If WEP authentication is used,** circle one: **Open System**, **Shared Key, or Auto**.

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

  - **WEP Encryption key size**. Choose 64-bit or 128-bit. The encryption key size must be the same for the wireless adapters and the wireless router.
  - **Data encryption (WEP) keys**. There are two ways to create WEP data encryption keys.
    - **Passphrase method**. ______________________________ These characters *are* case-sensitive. Enter a word or group of printable characters and click **Generate Keys**. Not all wireless devices support the passphrase method.
    - **Manual method**. These values *are not* case-sensitive. For 64-bit WEP, enter 10 hex digits (any combination of 0-9 or a-f). For 128-bit WEP, enter 26 hex digits.

  Key 1: ___________________________________

  Key 2: ___________________________________

  Key 3: ___________________________________

  Key 4: ___________________________________

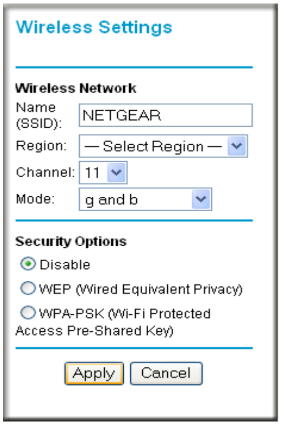
- If WPA-PSK or WPA2-PSK Authentication is Used:
  - **Passphrase**: ______________________________ These characters *are* case-sensitive. Enter a word or group of printable characters.

Use the procedures described in the following sections to configure the WGT624 v4. Store this information in a safe place.

Viewing or Change Wireless Settings

To view or change wireless settings:

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



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 11

Mode: g and b

Security Options

● Disable

○ WEP (Wired Equivalent Privacy)

○ WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)

Figure 2-1

3. View or enter the wireless settings for the router.

- **Wireless Network Name (SSID).** The default SSID is NETGEAR. It is a good idea to change this to a name that you can easily recognize in case there are other wireless networks in your area. You can enter up to 32 alphanumeric characters.

> **Note:** The network name (SSID) is case-sensitive. If NETGEAR is the network name (SSID) in your wireless router, you must enter NETGEAR in your computer’s wireless settings. Typing nETgear will not work.

- **Region.** The region where you are located. The Smart Wizard prompts for this during installation. It may not be legal to operate the wireless features of the wireless router in a region other than one of those identified in this field.
- **Channel.** The channel determines the operating frequency. The default channel is 11.

You need to change the channel only if you have interference problems with another nearby wireless router or access point. If this is the case, select a channel that is not being used by any other wireless networks within several hundred feet of your wireless router. For a link to more information on the wireless channel frequencies, see "Wireless Communications" in Appendix B.

- **Mode.** The data communications protocol that the router will use. You can select Auto 108 Mbps, g only, or g and b. The g only option dedicates the wireless router to communicating with the higher bandwidth 802.11g wireless devices exclusively. The g and b mode provides backward compatibility with the slower 802.11b wireless devices while still enabling 802.11g communications. The Auto 108 Mbps mode works with 802.11g, 802.11b, and NETGEAR 108 Mbps devices.
- **Security Options:** For initial set up and test, leave or set Security Options to None. For more information about Security Options, see "Understanding Wireless Security" on page 2-6.

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

Set up the wireless adapter for each computer that will connect to the router with the same SSID and wireless channel as the router. The SSID for the wireless adapters must match the SSID for the router or you will not get a wireless connection.

Test each computer to make sure that it can connect wirelessly to the router and is able to obtain an IP address by DHCP from the wireless router.

After your computers can connect wirelessly to the wireless router, then you can set up wireless security for your network.

Understanding Wireless Security

⚠ **Warning:** Indoors, computers can connect over 802.11g wireless networks at a maximum range of up to 300 feet. Such distances can allow for others outside of your immediate area to access your network.

To protect your network from unauthorized access, use the security features of your wireless equipment.

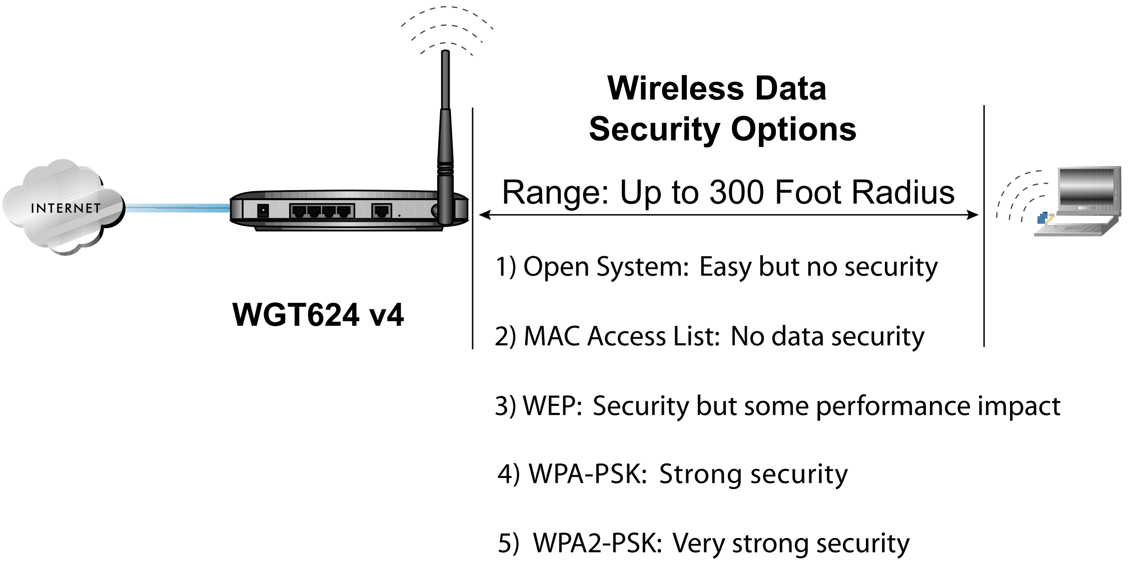

INTERNET
WGT624 v4
Wireless Data Security Options
Range: Up to 300 Foot Radius
1) Open System: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but some performance impact
4) WPA-PSK: Strong security
5) WPA2-PSK: Very strong security

Figure 2-2

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

- **Restrict access based on MAC (Media Access Control) address.** You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WGT624 v4. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn off the broadcast of the wireless network name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network “discovery” feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.

- **Wired Equivalent Privacy (WEP) data encryption.** Provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.
- **Wi-Fi Protected Access—Pre-Shared Key (WPA-PSK** and **WPA2-PSK).** Provide strong data security. WPA-PSK and WPA2-PSK will block eavesdropping. Because these are new standards, wireless device driver and software availability may be limited.
- **Turn off the wireless LAN.** If you disable the wireless LAN, wireless devices cannot communicate with the router at all. You might choose to turn off the wireless the LAN when you are away and the others in the household all use wired connections.

Wireless Security Options

The following table identifies the basic wireless security options on the Wireless Settings page. For a link to a full explanation of these standards, see "Wireless Communications" in Appendix B.

Wireless Security Option Field	Description
None	No wireless security.
WEP	WEP offers the following options: • Open System With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the WGT624 v4 does perform 64- or 128-bit data encryption but does not perform authentication. • Shared Key Shared Key authentication encrypts the SSID and data. Not all wireless adapter configuration utilities support passphrase key generation. • Auto The wireless router automatically detects whether Open System or Shared Key is used.
WPA-PSK WPA2-PSK	• WPA-Pre-shared Key *does* perform authentication. • WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption and WPA2-PSK uses AES (Advanced Encryption Standard) data encryption. Both dynamically change the encryption keys, making them nearly impossible to circumvent.

WEP Wireless Security

Note: Before setting up wireless security, verify that your wireless connections are set up and working. See "Setting Up Your Wireless Connections" on page 2-2.

When you are setting up wireless security, these guidelines will help make the process simpler and easier:

- Use an Ethernet cable to connect your computer to the router when you are setting up or changing wireless settings. If you are connected wirelessly and you set up the wireless security, you will lose your wireless connection when you apply the change.
- Remember to note what your wireless settings are. For help keeping track of them, see "Information to Gather Before Changing the Wireless Settings" on page 2-3.

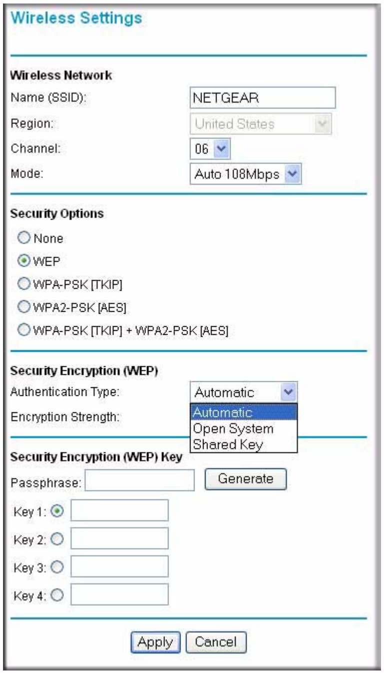
Note: For instructions for configuring wireless computers or personal digital assistants (PDAs) for WEP, see the documentation for the product you are using.

Setting Up WEP

To set up Wired Encryption Protocol (WEP) wireless security:

1. Log in to the WGT624 v4 wireless router at its default LAN address of *http://192.168.1.1* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless Settings link in the Setup section of the main menu.

3. In the Security Options section, select WEP. The WEP options display.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: 06

Mode: Auto 108Mbps

Security Options

○ None

● WEP

○ WPA-PSK [TKIP]

○ WPA2-PSK [AES]

○ WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength:

Security Encryption (WEP) Key

Passphrase:

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Figure 2-3

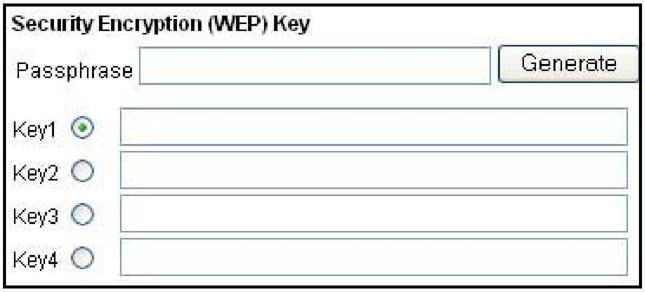
4. Select the Authentication Type.

The default setting is Automatic, which usually works. If it does not, select Open System or Shared Key. Check your wireless card’s documentation to see which method to use.

Note: 64-bit WEP encryption strength is sometimes referred to as 40-bit encryption.

5. From the Security Encryption drop-down list, select the WEP encryption strength.

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



Security Encryption (WEP) Key

Passphrase

Key1 ●

Key2 ○

Key3 ○

Key4 ○

Figure 2-4

- Automatic. Enter a word or group of printable characters for the Passphrase, and then click Generate. The passphrase is case-sensitive; NETGEAR is not the same as nETgear. The four key boxes will be automatically populated with key values.
- Manual. Select which of the four keys will be active and enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F).

See "Wireless Communications" in Appendix B for a link to a document on the NETGEAR Web site that contains a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

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

Tip: If you were connected wirelessly to the router, you lost the wireless connection when you clicked Apply. Now you must change the wireless security settings for your computer to match the router settings. Then you will be able to connect to the router.

WPA-PSK or WPA2-PSK Wireless Security

➡ **Note:** Before setting up wireless security, verify that your wireless connections are set up and working. See “Setting Up Your Wireless Connections” on page 2-2.

When you are setting up wireless security, these guidelines will help make the process simpler and easier:

- Use an Ethernet cable to connect your computer to the router when you are setting up or changing wireless settings. If you are connected wirelessly and you set up the wireless security, you will lose your wireless connection when you apply the change.
- Remember to note what your wireless settings are. For help keeping track of them, see “Information to Gather Before Changing the Wireless Settings” on page 2-3.

Wireless Adapter Compatibility

➡ **Note:** For instructions for configuring wireless computers or personal digital assistants (PDAs) for WPA-PSK, see the documentation for the product you are using.

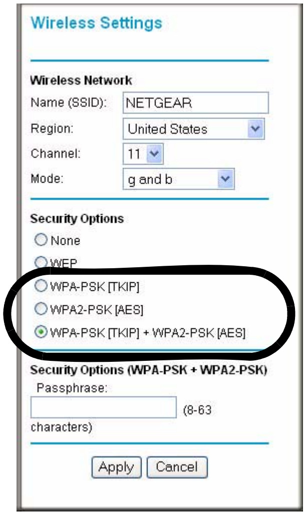
If you want to use WPA or WPA2, first make sure that the computers or devices that will connect to your router are able to use this type of wireless security. Each computer or device will need:

- A configuration utility that supports WPA or WPA2 for the wireless adapter.
- Client software that supports WPA or WPA2. Windows XP Service Pack 2 and Windows XP Service Pack 1 with the WPA patch do include the client software that supports WPA.
- The wireless adapter hardware and driver must also support WPA or WPA2.

Setting Up WPA-PSK or WPA2-PSK

To set up WPA-PSK or WPA2-PSK wireless security for the WGT624 v4 wireless router:

1. Click Wireless Settings in the Setup section of the main menu.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: 11

Mode: g and b

Security Options

○ None

○ WEP

○ WPA-PSK [TKIP]

○ WPA2-PSK [AES]

● WPA-PSK [TKIP] + WPA2-PSK [AES]

Security Options (WPA-PSK + WPA2-PSK)

Passphrase: (8-63 characters)

Figure 2-5

2. Select the security option that you want to use:
   - **WPA-PSK [TKIP].** Only computers or devices that use WPA-PSK [TKIP] will be able to connect to the router. WPA2-PSK [AES] devices cannot connect.
   - **WPA2-PSK [AES].** Only computers or devices that use WPA2-PSK [AES] will be able to connect to the router.WPA-PSK [TKIP] devices cannot connect.
   - **WPA-PSK [TKIP] + WPA2-PSK [AES]**. This option is recommended, since it is compatible with a greater number of computers and devices.
3. Enter a word or group of 8-63 printable characters in the Passphrase box.
4. Click **Apply** to save your settings.

> **Tip:** If you were connected wirelessly to the router, you lost the wireless connection when you clicked Apply. Now you must change the wireless security settings for your computer to match the router settings. Then you will be able to connect to the router.

Restricting Wireless Access by MAC Address

To restrict access based on MAC addresses:

1. Log in to the WGT624 v4 wireless router at its default LAN address of *http://*192.168.1.1 with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

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

2. Click the Wireless Settings link in the Advanced section of the main menu.
3. From the Wireless Settings page, click **S**etup Access List. The Wireless Card Access Setup page opens:

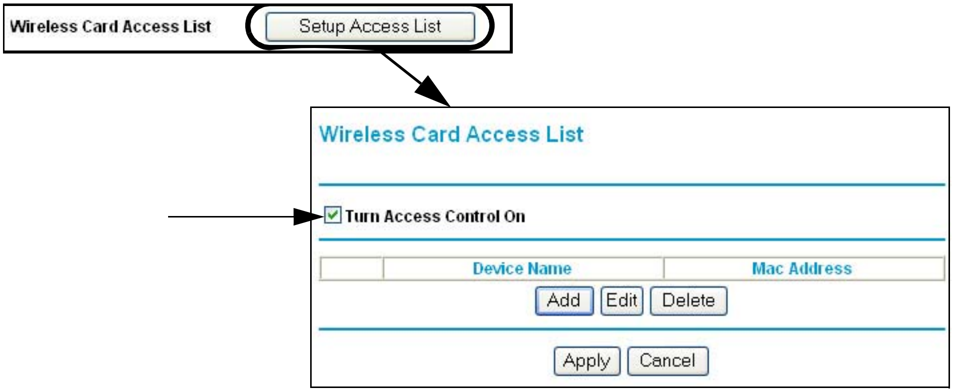
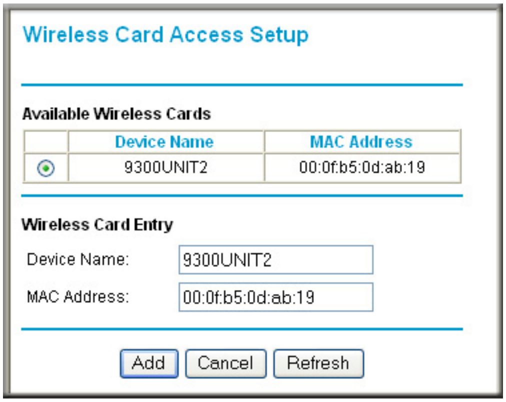


Figure 2-6

4. Select the Turn Access Control On check box.

5. Click Add to add a wireless device to the wireless access control list. The Available Wireless Cards list displays.



Wireless Card Access Setup

Available Wireless Cards

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

Wireless Card Entry

Device Name: 9300UNIT2

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

Figure 2-7

6. In the Available Wireless Cards list, either select from the list of cards the WGT624 v4 has found in your area, or enter the MAC address and device name for a device you plan to use. You can usually find the MAC address printed on the wireless adapter.

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

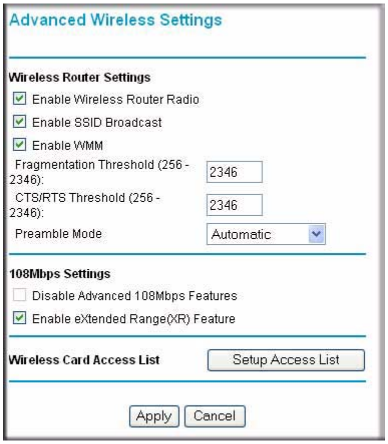
7. Click Add to add this wireless device to the Wireless Card Access list. The screen changes back to the list screen. Repeat these steps for each additional device you wish to add to the list.
8. Repeat steps 5-7 for each additional device you wish to add to the list.
9. Be sure to click **Apply** to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

Now, only devices on this list will be allowed to wirelessly connect to the WGT624 v4.

Advanced Wireless Settings

Log in to the WGT624 v4 wireless router at its default LAN address of *http://*192.168.1.1 with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

To go to advanced wireless settings, click the Wireless Settings link in the Advanced section of the main menu. The Advanced Wireless Settings page appears:



Advanced Wireless Settings

Wireless Router Settings

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

☑ Enable WMM

Fragmentation Threshold (256 - 2346): 2346

CTS/RTS Threshold (256 - 2346): 2346

Preamble Mode: Automatic

108Mbps Settings

☐ Disable Advanced 108Mbps Features

☑ Enable eXtended Range(XR) Feature

Wireless Card Access List

Figure 2-8

- **Enable Wireless Router Radio.** If you disable the wireless router radio, wireless devices cannot connect to the WGT624 v4.
- **Enable SSID Broadcast.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network ‘discovery’ feature of some products such as Windows XP.
- **Enable WMM.** Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS, are assigned to the best-effort category, which receives a lower priority than voice and video.

  To receive the benefits of WMM QoS:

  - The application must support WMM.
  - You must enable WMM in your WGT624 v4 wireless router.
  - You must enable WMM in the wireless adapter in your computer.

- **Wireless Card Access List.** When the Trusted PCs Only radio button is selected, the WGT624 v4 checks the MAC address of the wireless station and allows only connections to computers identified on the trusted computers list.
- **108Mbps Settings.**
  - **Disable Advanced 108Mbps Features**: Disables data compression, packet bursting, and large frame support.

    > **Note:** If the current wireless mode is Auto 108 Mbps, then this feature cannot be changed. It is to ensure the highest throughput when in Auto 108 Mbps wireless mode.

  - **Enable eXtended Range**: Provides significantly longer range than basic 802.11, maintaining connectivity even when signals have to pass through dense walls, floors, or other barriers. XR products require no additional configuration and are fully compatible with standard 802.11 technologies.

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

Chapter 3
Content Filtering

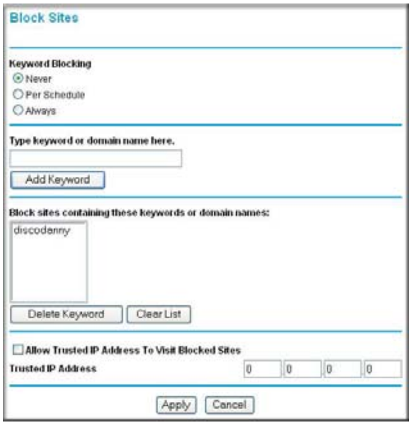
This chapter describes how to use the WGT624 v4 wireless router content filtering features to protect your network.

The WGT624 v4 wireless router provides you with Web content filtering options, plus browser activity reporting and instant alerts via e-mail. You 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.

Log in to the router at its default LAN address of **http://www.routerlogin.net** with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up. The content filtering features are on the router's main menu.

Blocking Access to Internet Sites

You can restrict access based on Web addresses and web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites page is shown below:



Block Sites

Keyword Blocking
● Never
○ Per Schedule
○ Always

Type keyword or domain name here.

Block sites containing these keywords or domain names:
discodanny

□ Allow Trusted IP Address To Visit Blocked Sites
Trusted IP Address 0 0 0 0

Figure 3-1

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

- To add a keyword or domain, type it in, click Add Keyword, and then click **Apply**.
- To delete a keyword or domain, select it from the list, click Delete Keyword, and then click **Apply**.
- To specify a trusted user, enter that computer’s IP address in the Trusted User box and then click **Apply**. You may specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.

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 websites with other domain suffixes (such as .edu or .gov) can be viewed.
- If you want to block all Internet browsing access during a scheduled period, enter the keyword “.” and set the schedule in the Schedule page.

Blocking Services (Port Filtering)

You can block the use of certain Internet services by computers on your network. This is called services blocking or port filtering.

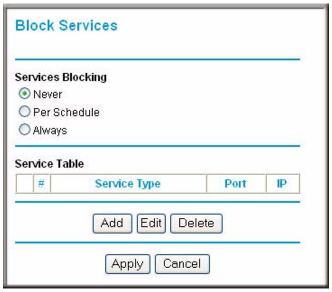
Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players’ moves.

When a computer on your network sends a request for service to a server computer on the Internet, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

Blocking Access to Internet Services

To block access to Internet services:

1. Click Block Access to go to the Block Services page:



Block Services

Services Blocking
● Never
○ Per Schedule
○ Always

Service Table

	#	Service Type	Port	IP

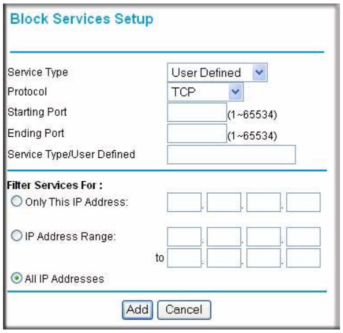
Figure 3-2

2. Select the Services Blocking setting that you want:
   - **Never.** Do not block services.
   - **Per Schedule.** Block services based on the schedule. Make sure that you specify a time period in the Schedule page.
   - **Always.** Always block services.
3. Click **Apply**.

Adding a Service to be Blocked

To specify a service for blocking:

1. On the Block Sites page, click Add. The Block Services Setup page appears:



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

Figure 3-3

2. From the Service Type drop-down list, select the application or service to be allowed or blocked.

   The list displays several common services, but you are not limited to these choices.

3. To add any additional services or applications that do not already appear, select User Defined. See "Creating a User-Defined Service Type" on page 3-4.

4. You can use the Filter Services for settings to block the specified service for a single computer, a range of computers (having consecutive IP addresses), or all computers on your network.

Creating a User-Defined Service Type

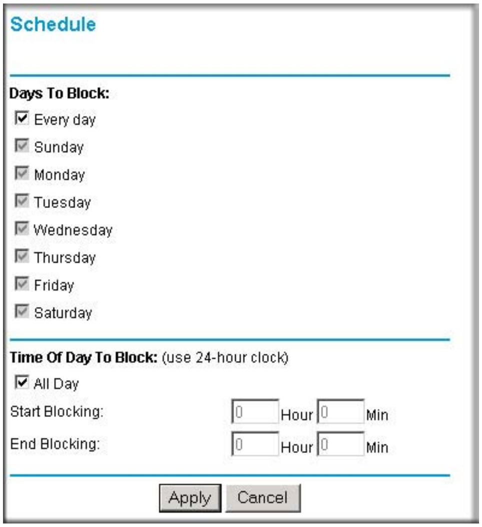
You will need to enter the protocol, starting point, and ending point for the service type.

- **Protocol.** If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select TCP/UDP.
- **Starting Point and Ending Point.** Enter the starting port and ending port numbers. If the application uses a single port number, enter that number in both boxes.

  To define a service, you must determine which port number or range of numbers the application uses. 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.
- **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 Blocking

You can specify when blocking will be enforced. The Schedule page is shown below:



Schedule

Days To Block:

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

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

☑ All Day

Start Blocking: 0 Hour 0 Min

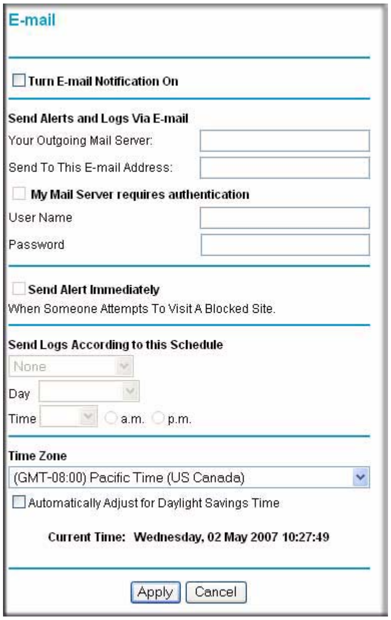
End Blocking: 0 Hour 0 Min

Figure 3-4

1. Use the check boxes to create a schedule for blocking content:
   - **Days To Block.** Select days to block by selecting the appropriate check boxes. Select **Every Day** to select the check boxes for all days.
   - **Time Of Day To Block.** Select a start and end time in 24-hour format. Select **All Day** for 24-hour blocking.
2. Click **Apply**.
3. Select your time zone in the E-Mail page. For details, see the following section, "E-Mail Alerts and Web Access Log Notifications".

E-Mail Alerts and Web Access Log Notifications

The E-mail page is shown below:



E-mail

□ Turn E-mail Notification On

Send Alerts and Logs Via E-mail

Your Outgoing Mail Server:

Send To This E-mail Address:

□ My Mail Server requires authentication

User Name

Password

□ Send Alert Immediately

When Someone Attempts To Visit A Blocked Site.

Send Logs According to this Schedule

None

Day

Time ○ a.m. ○ p.m.

Time Zone

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

□ Automatically Adjust for Daylight Savings Time

Current Time: Wednesday, 02 May 2007 10:27:49

Figure 3-5

To set up e-mail alerts and log notifications:

1. To receive logs and alerts by email, you must provide your email information
   - **Turn E-mail Notification On.** Select this check box if you want 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.
   - **My Mail Server requires authentication.** Select this check box if authentication is required, and enter the user name and password.
   - **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.

2. Specify whether or not you want alters or logs automatically sent to the specified e-mail address:

- **Send Alert Immediately.** Select this check box to receive immediate notification of attempted access to a blocked site.
- **Send Logs According to this Schedule.** Specifies how often to send the logs: None, Hourly, Daily, Weekly, or When Full.
  - None. Logs will not be sent. If you turned on e-mail notification, the alert will be sent but not the log.
  - Day for sending log. The day of the week to send the log. Relevant when the log is sent weekly or daily.
  - Time for sending log. The time of day to send the log. Relevant when the log is sent daily or weekly.

If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the 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.

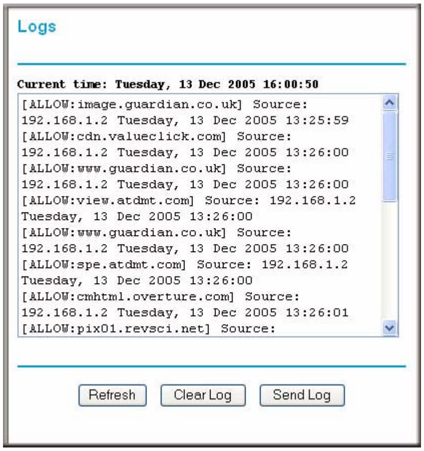
3. The wireless router uses Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. In order to localize the time for your log entries, you must specify your time zone:

- Time Zone. Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
- Automatically Adjust for Daylight Savings Time. Select this check box to automatically adjust for daylight savings time.

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

Viewing Logs of Web Access or Attempted Web Access

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



Current time: Tuesday, 13 Dec 2005 16:00:50

```
[ALLOW:image.guardian.co.uk] Source:
192.168.1.2 Tuesday, 13 Dec 2005 13:25:59
[ALLOW:cdn.valueclick.com] Source:
192.168.1.2 Tuesday, 13 Dec 2005 13:26:00
[ALLOW:www.guardian.co.uk] Source:
192.168.1.2 Tuesday, 13 Dec 2005 13:26:00
[ALLOW:view.atdmt.com] Source: 192.168.1.2
Tuesday, 13 Dec 2005 13:26:00
[ALLOW:www.guardian.co.uk] Source:
192.168.1.2 Tuesday, 13 Dec 2005 13:26:00
[ALLOW:spe.atdmt.com] Source: 192.168.1.2
Tuesday, 13 Dec 2005 13:26:00
[ALLOW:cmhtml.overture.com] Source:
192.168.1.2 Tuesday, 13 Dec 2005 13:26:01
[ALLOW:pix01.revsci.net] Source:
```

Figure 3-6

Log entries are described in Table 3-1, and Log action buttons are described in Table 3-2.

Table 3-1. Log Entry Descriptions

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

Table 3-2. Log Action Buttons

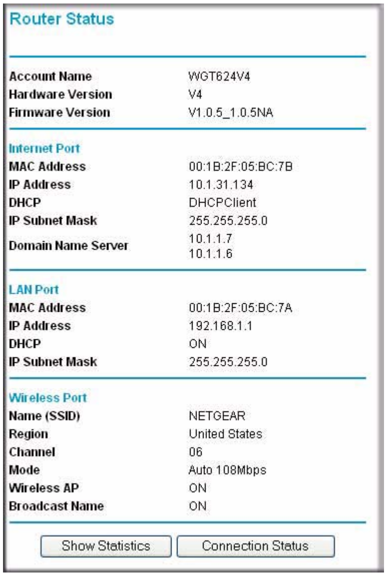
Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to email the log immediately.

Chapter 4
Maintenance

This chapter describes how to use the maintenance features of your WGT624 v4 wireless router. These features can be found under the Maintenance heading in the router's main menu.

Viewing the Router Status

The Router Status menu provides status and usage information. From the Maintenance section of the main menu, select Router Status to view the Router Status screen:



Router Status

Account Name	WGT624V4
Hardware Version	V4
Firmware Version	V1.0.5_1.0.5NA
Internet Port	
MAC Address	00:1B:2F:05:BC:7B
IP Address	10.1.31.134
DHCP	DHCPClient
IP Subnet Mask	255.255.255.0
Domain Name Server	10.1.1.7 10.1.1.6
LAN Port	
MAC Address	00:1B:2F:05:BC:7A
IP Address	192.168.1.1
DHCP	ON
IP Subnet Mask	255.255.255.0
Wireless Port	
Name (SSID)	NETGEAR
Region	United States
Channel	06
Mode	Auto 108Mbps
Wireless AP	ON
Broadcast Name	ON

Figure 4-1

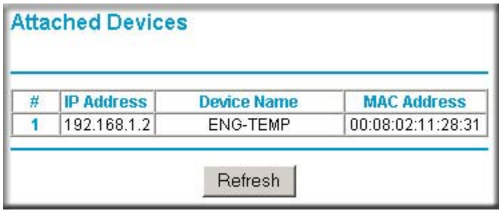
This screen shows the following fields:

Table 4-1. Router Status Fields

Field	Description
Account Name	The host name assigned to the router.
Firmware Version	The router firmware version.
Internet Port	Router Internet (WAN) port,
MAC Address	The Media Access Control address being used by the Internet (WAN) port of the router.
IP Address	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 DHCP is set to None, the router uses 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	The IP subnet mask used by the Internet (WAN) port of the router.
Domain Name Server	The address of the current domain name server.
LAN Port	Router local (LAN) port.
MAC Address	The Media Access Control address being used by the LAN port of the router.
IP Address	The IP address being used by the Local (LAN) port of the router. The default is 192.168.1.1.
DHCP	Identifies if the router's built-in DHCP server is active for the LAN attached devices.
IP Subnet Mask	The IP subnet mask used by the Local (LAN) port of the router. The default is 255.255.255.0
Wireless Port	Router wireless port.
Name (SSID)	The wireless network name (SSID) used by the wireless port of the router. The default is NETGEAR.
Region	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	The channel the wireless port is using. See the link in "Wireless Communications" in Appendix B for information about the frequencies used on each channel.
Mode	The current mode (g & b, g only, or Auto 108 Mbps).
Wireless AP	Indicates if the access point feature of the router is enabled. If it is disabled, then wireless devices cannot connect to the network.
Broadcast Name	Indicates if the wireless router is broadcasting its SSID.

Viewing a List of Attached Devices

The Attached Devices page 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:



Attached Devices

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

Figure 4-2

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

Note: Rebooting the router empties the table data until the router rediscovers the devices. To force the router to look for attached devices, click **Refresh**.

Upgrading the Router Firmware

The router firmware is stored in FLASH memory, and can be upgraded as new firmware is released by NETGEAR. The upgrade process will typically take about one minute. Additionally, some upgrades will require you to reset your router to its factory default settings.

Note: Be sure to check the NETGEAR website for documentation updates, which are available at *http://www.netgear.com/support*.

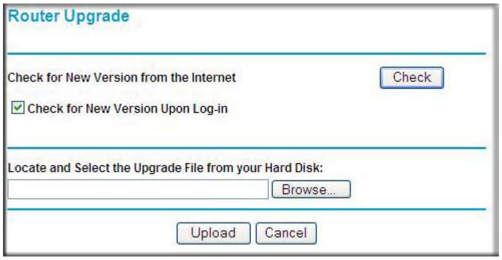
To upgrade the router firmware:

1. Before you begin, make sure that you have:

- A computer with a Web browser that supports HTTP uploads. For example, you can use Microsoft Internet Explorer or Netscape Navigator 4.0 or later.

- Your router configuration settings (see "Configuration File Management" on page 4-5). After some firmware updates you will need to reset the wireless router to its factory default settings. If this is the case then you will need to configure the router.

2. Connect to the router, and select Router Upgrade from the router's main menu.



Router Upgrade

Check for New Version from the Internet

☑ Check for New Version Upon Log-in

Locate and Select the Upgrade File from your Hard Disk:

Figure 4-3

Warning: When uploading software to the wireless router, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software.

3. To check for new firmware, click Check.If the wireless router finds new firmware is available, follow the onscreen prompts to download and install the new firmware.

4. To upload firmware from your computer onto the router, click Browse in the Router Upgrade page, and browse to the location of the binary (.chk) upgrade file.

5. Click Upload.

When the upload is complete, your router will automatically restart.

Note: In some cases, you may need to reset to factory default and reconfigure the router after upgrading.

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) onto a computer, retrieved (restored) from the computer, or cleared to the factory default settings.

From the Maintenance section of the main menu, click Backup Settings.

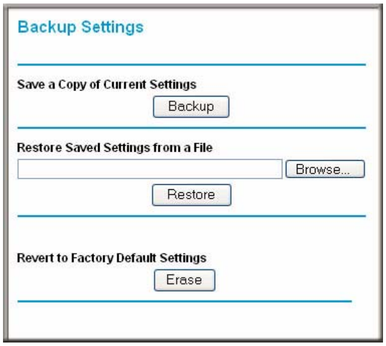

Backup Settings
Save a Copy of Current Settings
Backup
Restore Saved Settings from a File
Browse...
Restore
Revert to Factory Default Settings
Erase

Figure 4-4

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

Backing Up and Restoring the Configuration

You can save and retrieve a file containing your router’s configuration settings.

- To save your settings:
  Click Backup. Your browser will extract the configuration file from the router and prompt you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as pacbell.cfg.
- To restore your settings from a saved configuration file:
  Enter the full path to the file on your computer or click Browse to browse to the file. When you have located it, click Restore to send the file to the router. The router will then reboot automatically.

Erasing the Configuration

You can restore the router to the factory default settings with the Erase function. 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.

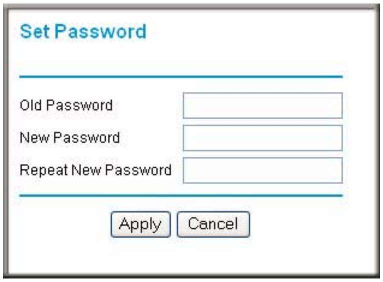
- To erase the configuration, click Erase on the Backup Settings page.
- To restore the factory default configuration settings without knowing the login password or IP address, use the Reset button on the rear panel of the router. See "Restoring the Default Configuration and Password" on page 6-7.

Changing the Administrator Password

The default password for the router is **password**. NETGEAR recommends that you change this password to a more secure password.

To change the administrator password:

1. From the router's main menu, below the Maintenance heading, select Set Password.



Set Password

Old Password	
New Password	
Repeat New Password	

Figure 4-5

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

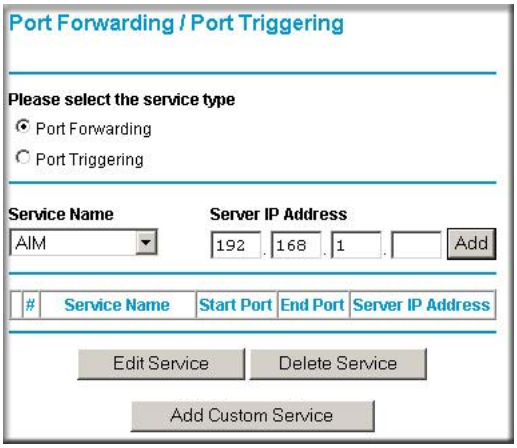
Chapter 5
Advanced Configuration

This chapter describes how to configure the advanced features of your WGT624 v4 wireless router. These features are listed under the Advanced heading in the router's main menu.

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 page.

From the Advanced section of the main menu, click Port Forwarding / Port Triggering to view the port forwarding page.



Port Forwarding / Port Triggering

Please select the service type

● Port Forwarding

○ Port Triggering

Service Name: AIM

Server IP Address: 192 . 168 . 1 .

#	Service Name	Start Port	End Port	Server IP Address

Figure 5-1

Note: If you are unfamiliar with networking and routing, see "Internet Networking and TCP/IP Addressing" in Appendix B," for a link to a tutorial that will help you become more familiar with the terms and procedures used in this manual.

You can 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.

Before starting, determine which type of service, application or game you will provide and the IP address of the computer that will provide each service. Be sure the computer's IP address never changes. To configure port forwarding to a local server:

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

Adding a Port-Forwarding Custom Service

To define a service, game, or application that does not appear in the Service Name 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. Click Add Custom Service.
2. Enter the first port number in an unused Starting Port box.
3. To forward only one port, enter it again in the Ending Port box. To specify a range of ports, enter the last port to be forwarded in the End Port box.
4. Enter the IP address of the local server in the corresponding Server IP Address box.
5. Type a name for the service.
6. Click **Apply**.

Editing or Deleting a Port-Forwarding Entry

To edit or delete a port forwarding entry:

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

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, users can access your Web server by directing the browser to http://172.16.1.23. You can view the assigned IP address in the Maintenance Status page, 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.

Network Computer Gaming 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 Service Name 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 have already configured one computer to play Hexen II (using port 26900), the second computer's port number would be 26901, and the third computer would be 26902.
4. Type the same port number in the End Port box that you typed in the Start Port box.
5. Type the IP address of the additional computer in the Server IP Address box.
6. Click **Apply**.

Some online games and videoconferencing applications are incompatible with NAT. The WGT624 v4 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 videoconferencing host, enter its IP address as the default.

Using Port Triggering

Port triggering is an advanced feature that allows you to dynamically open inbound ports on the basis of outbound traffic on different ports. This feature can be used for gaming and other Internet applications.

Port forwarding can typically be used to enable similar functionality, but it is static and has some limitations. Ports will be open to traffic from the Internet until the port-forwarding rule is removed. Additionally, port forwarding does not work well for some applications when your WAN IP address is assigned by DHCP, and is changed frequently. 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.

Port triggering monitors outbound traffic. When the gateway 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.

Once configured, operation is as follows:

1. A computer makes an outgoing connection using a port number defined in the Port Triggering table.
2. The wireless router records this connection, opens the INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the computer.
3. The remote system receives the computer's request, and responds using a different port number.
4. The wireless router matches the response to the previous request, and forwards the response to the computer.

Without port triggering, this response would be treated as a new connection request rather than a response. As such, it would be handled in accordance with the port forwarding rules.

Note: Only one computer can use a port triggering application at any time.

After a computer has finished using a port Triggering application, there is a time-out period before the application can be used by another computer. This is required because the wireless router cannot be sure when the application has terminated.

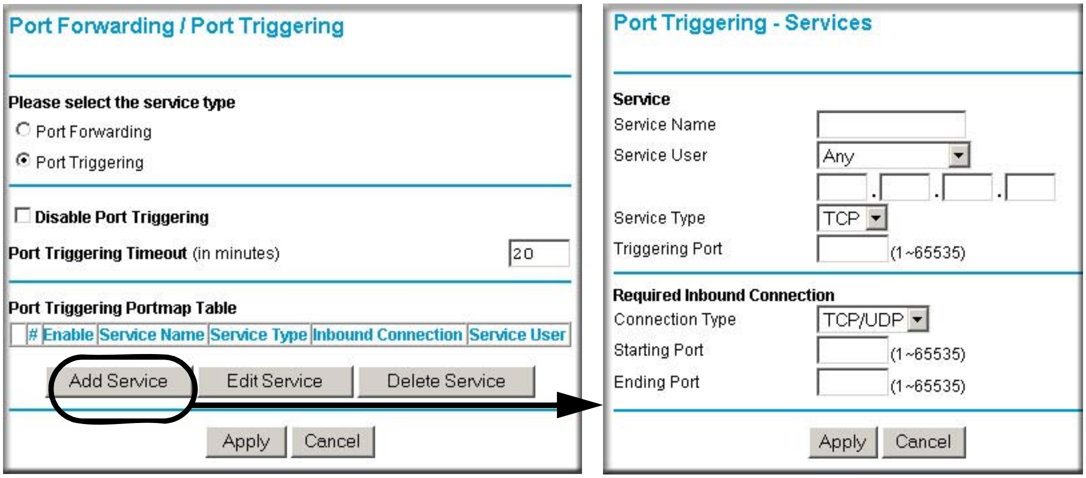
Port Triggering Menu

The Port Triggering Portmap Table lists the current port triggering services:

- **Enable.** Indicates if the rule is enabled or disabled. Generally, there is no need to disable a rule unless it interferes with some other function, such as port forwarding.
- **Service Name.** The name assigned to this service.
- **Service Type.** Either TCP or UDP.
- **Inbound Connection—**indicates the type of inbound connection (TCP/UDP, TCP, or UDP) and the port range.
- **Service User**—indicates who can use the service on the network.

Adding a New Service

To add a new service, click Add Service, and then enter the following data.



Port Forwarding / Port Triggering

Please select the service type

○ Port Forwarding

● Port Triggering

□ Disable Port Triggering

Port Triggering Timeout (in minutes) 20

Port Triggering Portmap Table

#	Enable	Service Name	Service Type	Inbound Connection	Service User

Port Triggering - Services

Service

Service Name

Service User: Any

Service Type: TCP

Triggering Port (1~65535)

Required Inbound Connection

Connection Type: TCP/UDP

Starting Port (1~65535)

Ending Port (1~65535)

Figure 5-2

1. Enter service name in the Service Name box (for example, the name of the application)
2. Select Any or Single address from the Service User drop-down list. The default value (Any) will allow everyone on the network to use the service. If you select Single address, enter the IP address of the computer that will be allowed to use the service.

3. Select the service type (TCP or UDP) from the Service Type drop-down list.
4. Enter the *outbound* port number in the Triggering Port box.
5. Enter the inbound connection port information:
   a. Connection type (TCP/UDP, TCP, or UDP)
   b. Starting port
   c. Ending port

   For inbound connection information, see the game or applications manual or the product's support website.

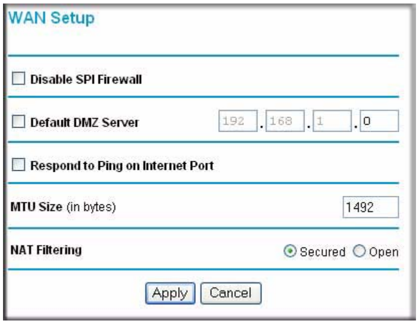
Editing or Deleting a Service

To edit an existing service:

1. From the Port Triggering page, select the service you want to edit from the list of services in the Port Triggering Portmap Table.
2. Click Edit Service or Delete Service, as required.
3. If editing, change the service information on the Port Triggering - Services page, as described in "Adding a New Service" on page 5-5, and then click **Apply.**

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.



WAN Setup

□ Disable SPI Firewall

□ Default DMZ Server 192 . 168 . 1 . 0

□ Respond to Ping on Internet Port

MTU Size (in bytes) 1492

NAT Filtering ● Secured ○ Open

Figure 5-3

The WAN setup options are explained below:

- Disable SPI Firewall.

  Normally, this option should be enabled, so that your local network will be protected by the stateful packet inspection (SPI) firewall included in the wireless router. However, certain communications functions like VPN may require turning off the SPI feature.

➡	**Note:** When SPI firewall is disabled, you must use the Passive mode in the computer FTP client to connect to the FTP server.

- Default DMZ Server.

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

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

  Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the 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.

- NAT Filtering.

  This determines how your router handles inbound traffic. The Secured option provides a secure firewall to protect the computers on the LAN from attacks from the Internet, but it may cause some Internet games, point-to-point applications, or multimedia applications not to work. The Open option provides less protection, but allows almost all Internet applications to work.

- Assigning a Default DMZ Server. See "Assigning a Default DMZ Server" on page 5-8.

- Respond to a Ping on the Internet WAN Port.

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

- Setting the MTU Size. In most cases it is not necessary to set the MTU size. See "Setting the MTU Size" on page 5-8.

Assigning a Default DMZ Server

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

1. Click WAN Setup on the Advanced section of the main menu.
2. Type the IP address for that server. To remove the default DMZ server, clear the Default DMZ Server check box.
3. Click **Apply**.

Setting the MTU Size

The default MTU size does not usually need to be changed. The normal maximum transmit unit (MTU) value for most Ethernet networks is 1500 bytes. For some ISPs, particularly some using PPPoE, you may need to reduce the MTU. You should not do this unless you are sure it is necessary for your ISP.

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.

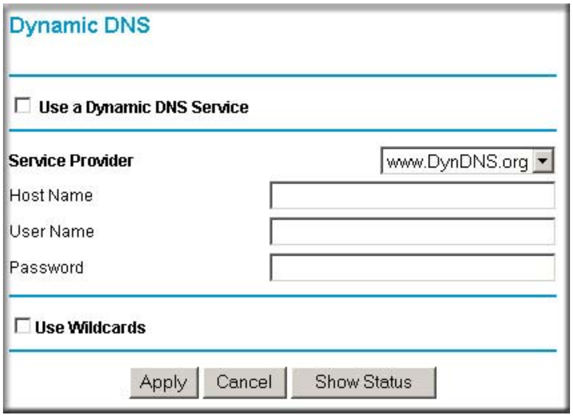
Using a Dynamic DNS Service

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 that will allow you to register your domain to their IP address, and will forward traffic directed at your domain to whatever your current IP address happens to be.

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 wireless router's main menu, under Advanced, click Dynamic DNS.



Dynamic DNS

□ Use a Dynamic DNS Service

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

□ Use Wildcards

Figure 5-4

To configure dynamic DNS:

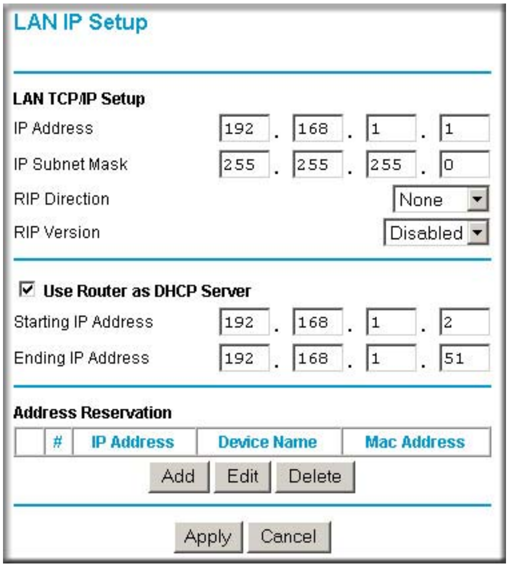
1. Register for an account with one of the dynamic DNS service providers whose names appear in the Select Service Provider box. For example, for dyndns.org, enter www.dyndns.org.
2. Select the "Use a Dynamic DNS Service" check box.
3. Select the name of your dynamic DNS Service Provider.
4. Type the Host Name (or domain name) that your dynamic DNS service provider gave you.
5. Type the User Name for your dynamic DNS account.
6. Type the Password (or key) for your dynamic DNS account.
7. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Use Wildcards check box to activate this feature.

For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org

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

Using LAN IP Setup Options

The LAN IP Setup feature allows configuration of LAN IP services such as DHCP and RIP. From the wireless router's main menu, under Advanced, click LAN IP Setup.



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

Figure 5-5

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

- LAN IP address—192.168.1.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable 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.

  – Both or Out Only: The router will broadcast its routing table periodically.

  – Both or In Only: The router will incorporate the RIP information that it receives.

  – None (default): The router 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, it is disabled.

  – 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 your computer is connected through the browser, you will be disconnected. You need run *ipconfig /release* and *ipconfig /renew* commands on your computer to reconnect to the router. You may need to restart your computer for the new IP address setting to take effect.

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 "Internet Networking and TCP/IP Addressing" in Appendix B" for a link to a tutorial that provides 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 selected.

Specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.1.2 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 information to any LAN device that requests DHCP:

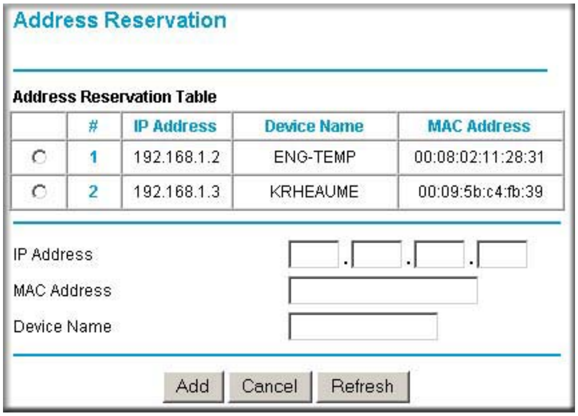
- An IP address from the range you have defined
- Subnet mask
- Gateway IP Address (the router's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Basic Settings page; otherwise, the router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Basic Settings page

Using Address Reservation

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

To reserve an IP address:

1. In the LAN IP Setup page, click **Add**.



Address Reservation

Address Reservation Table

	#	IP Address	Device Name	MAC Address
○	1	192.168.1.2	ENG-TEMP	00:08:02:11:28:31
○	2	192.168.1.3	KRHEAUME	00:09:5b:c4:fb:39

IP Address . . .

MAC Address

Device Name

Figure 5-6

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 page and paste it here. See “Viewing a List of Attached Devices” on page 4-3

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.

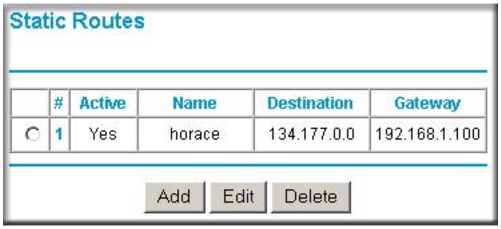
2. Click **Edit** or **Delete**.

How to Configure 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.

To add or edit a static route:

1. From the wireless router’s main menu, under Advanced, click Static Routes.

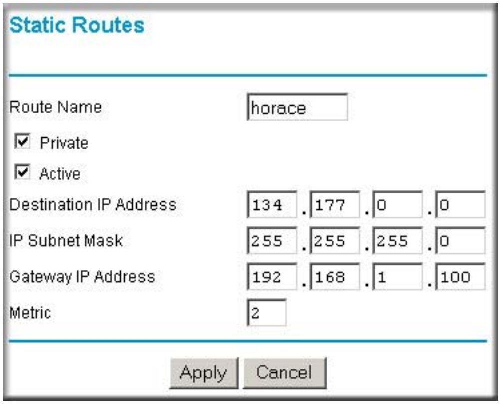


Static Routes

	#	Active	Name	Destination	Gateway
○	1	Yes	horace	134.177.0.0	192.168.1.100

Figure 5-7

2. Click Add. The following page opens:



Static Routes

Route Name: horace

☑ Private

☑ Active

Destination IP Address: 134 . 177 . 0 . 0

IP Subnet Mask: 255 . 255 . 255 . 0

Gateway IP Address: 192 . 168 . 1 . 100

Metric: 2

Figure 5-8

3. Type a route name for this static route in the Route Name box under the table. (This is for identification purpose only.)

4. If you want to limit access to the LAN only, select Private. The static route will not be reported in RIP.

5. Select Active to make this route effective.
6. Type the Destination IP Address of the final destination.
7. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type 255.255.255.255.
8. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.
9. 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.
10. Click **Apply** to have the static route entered into the table.

When to Use a Static Route

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 route was created to your local network for all 192.168.1.x addresses. With this configuration, if you try to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. The static route would look like Figure 5-8.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.0.x addresses.
- The Gateway IP Address fields specify 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.

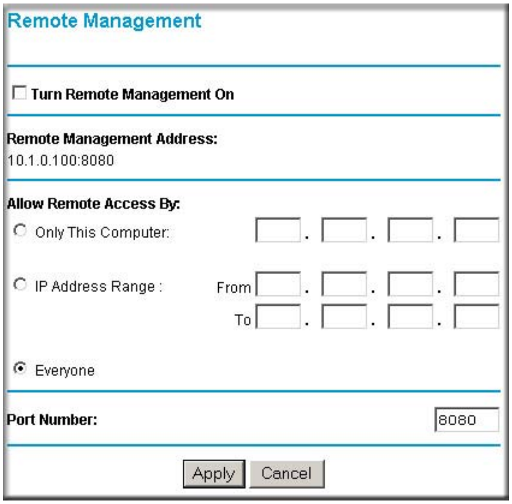
Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade, and check the status of your WGT624 v4 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 uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

To configure your router for remote management:

1. On the main menu, under the Advanced heading, select Remote Management.



Remote Management

□ Turn Remote Management On

Remote Management Address:
10.1.0.100:8080

Allow Remote Access By:

○ Only This Computer: [ ].[ ].[ ].[ ]

○ IP Address Range : From [ ].[ ].[ ].[ ]
To [ ].[ ].[ ].[ ]

● Everyone

Port Number: 8080

Figure 5-9

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

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

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

b. To allow access from a range of IP addresses on the Internet, select an IP address range. Enter a beginning and ending IP address to define the allowed range.

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

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

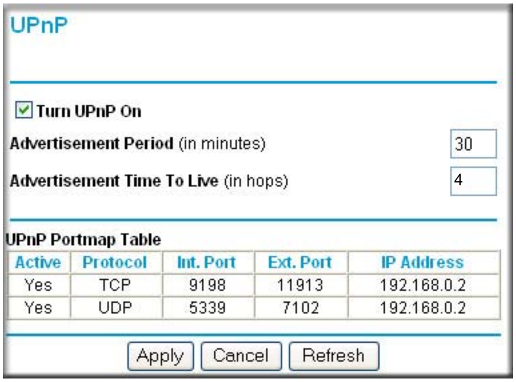
   Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The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

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): 30

Advertisement Time To Live (in hops): 4

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 5-10

- **Turn UPnP On:** UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.
- **Advertisement Period**: The Advertisement Period is how often the router 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 WGT624 v4 wireless router. After each problem description, instructions are provided to help you diagnose and solve the problem.

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

Basic Functioning

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

1. When power is first applied, verify that the Power LED is on.

2. After approximately 10 seconds, verify that:

   a. The Local port LEDs are lit for any local ports that are connected.

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

   b. The Wireless port LED is lit.

   c. The Internet port LED is lit.

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

Power LED Not On

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

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

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

LEDs Never Turn Off

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

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

- Cycle the power to see if the router recovers.
- Clear the router’s configuration and reset it 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.

Local or Internet Port LEDs Not On

If either the LAN LEDs or WAN LED 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 WAN 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.

Accessing the Wireless Router’s Main Menu

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

- Check the Ethernet connection between the computer and the router as described in the “Testing the LAN Path to Your Router” on page 6-5.
- 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. See “Preparing a Computer for Network Access” in Appendix B for a link to a document that describes how to find your computer’s IP address. Follow the instructions in that document to configure your computer.

> ➡ **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 autogenerated addresses have the subnet address 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 do not 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, check the following:

- When entering configuration settings, be sure to click **Apply** before exiting a page, or your changes are lost.
- Click Refresh or Reload 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.
2. Access the main menu of the router's configuration at **http://192.168.1.1**.
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 then reapply power to the cable or DSL modem.
4. When the modem's LEDs indicate that it has reacquired sync with the ISP, reapply power to your router.

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 page.
- Your ISP allows only one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case choose one of these options:

  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 page.

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. For help, see the link to the online document, "Preparing a Computer for Network Access" in Appendix B. Or, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

  If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address as described in "Preparing a Computer for Network Access" in Appendix B.

Troubleshooting a TCP/IP Network Using a Ping Utility

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

Testing the LAN Path to Your Router

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

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

1. From the Windows toolbar, click Start and select Run.
2. In the field provided, type ping followed by the IP address of the router, as in this example:
   ```
   ping 192.168.1.1
   ```
3. Click **OK**.

You should see a message like this one:

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

If the path is working, you see this message:

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

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

```
Request timed out
```

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

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in "Local or Internet Port LEDs 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. For help see the link to the online document in "Preparing a Computer for Network Access" in Appendix B.

– Check to see that the network address of your computer (the portion of the IP address specified by the 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 page.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single 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 4-6).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

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

1. Press and hold the Default Reset button until the Test LED turns on (about 5 seconds).
2. Release the Default Reset button, and then wait for the router to reboot.

Problems with Date and Time

To view the current date and time of day, select E-Mail below the Content Filtering heading on the main menu. 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, 2003. 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 then check the date and time.
- Time is off by one hour. Cause: The router does not automatically sense daylight savings time. On the E-Mail page, select or clear the check box marked “Adjust for Daylight Savings Time”.

Appendix A
Technical Specifications and Default Configuration

This appendix provides technical specifications for the WGT624 v4 wireless router.

Technical Specifications

The table below shows the technical specifications for the WGT624 v4 108 Mbps Wireless Router.

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):	12V DC @ 1 A output, 22W maximum
Physical Specifications	
Dimensions:	28 x 175 x 118 mm (1.1 x 6.89 x 4.65 in.)
Weight:	0.3 kg (0.66 lb)
Environmental Specifications	
Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	90% maximum relative humidity, noncondensing
Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B VCCI Class B EN 55 022 (CISPR 22), Class B

Interface Specifications

LAN:	10BASE-T or 100BASE-TX, RJ-45
WAN:	10BASE-T or 100BASE-TX, RJ-45
Wireless	
Radio Data Rates	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps Auto Rate Sensing
Frequency	2.4-2.5 GHz
Data Encoding:	Direct Sequence Spread Spectrum (DSSS)
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)
Encryption:	40-bit (also called 64-bit), 128-bit WEP data encryption, WPA-PSK(TKIP), and WPA2-PSK(AES)

Default Configuration Settings

You can use the reset button located on the back of your WGT624 v4 wireless router to reset all settings to their factory defaults. This is called a hard reset. To perform a hard reset, push and hold the reset button for 3 seconds. Your wireless router will return to the factory configuration settings shown in the table below.

Table A-1. Default Configuration Settings

Feature		Default Behavior
Smart Wizard		Disabled
Router Login		
	Router Login URL	http://www. routerlogin.net *or* http://www.routerlogin.com
	Login Name (case sensitive)	admin
	Login Password (case sensitive)	password
Internet Connection		
	WAN MAC Address	Use default hardware address
	MTU Size	1500
Local Network		
	Router LAN IP address (aka Gateway IP address)	192.168.1.1
	Router Subnet	255.255.255.0
	DHCP Server	Enabled
	Time Zone	GMT
	Time Zone Adjusted for Daylight Savings Time	Disabled
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (bars all unsolicited requests except for traffic on port 80, the http port)
	Outbound (communications going out to the Internet)	Enabled (all)

Table A-1. Default Configuration Settings (continued)

Feature		Default Behavior
Wireless		
	Wireless Communication	Enabled
	SSID Name	NETGEAR
	Security	Disabled
	Broadcast SSID	Enabled
	Transmission Speed	Auto[*]
	Country/Region	United States (in North America, otherwise varies by region)
	RF Channel	11 in North America, otherwise varies by region
	Operating Mode	Auto 108 Mbps in North America & Europe, otherwise varies by region
	Data Rate	Best
	Output Power	Full

[*]. 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.

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
Windows XP and Vista Wireless Configuration Utilities	*http://documentation.netgear.com/reference/enu/winzerocfg/index.htm*
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*

Index