# Reference Manual for the 108 Mbps Wireless Firewall Router WGT624 v3

NETGEAR

**NETGEAR**, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

202-10090-03 v.15
December 2005

## 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.

## EN 55 022 Declaration of Conformance

This is to certify that the WGT624 v3 108 Mbps Wireless Firewall 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 v3 108 Mbps Wireless Firewall 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.

## Certificate of the Manufacturer/Importer

It is hereby certified that the WGT624 v3 108 Mbps Wireless Firewall 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 v3 108 Mbps Wireless Firewall 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 v3 |
| **Publication Date:** | December 2005 |
| **Product Family:** | router |
| **Product Name:** | WGT624 v3 108 Mbps Wireless Firewall Router |
| **Home or Business Product:** | Home |
| **Language:** | English |
| **Publication Part Number:** | 202-10090-03 v.15 |

# Contents

# Chapter 1
# About This Manual

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

## Audience, Scope, Conventions, and Formats

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, Appendix B, "Related Documents" contains links to articles and tutorials on the NETGEAR Web site about basic computer network, Internet, firewall, and VPN technologies.

This guide uses the following typographical conventions:

**Table 1-1. Typographical Conventions**

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

This guide uses the following formats to highlight special messages:

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

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

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

This manual is written for the WGT624 v3 wireless router according to these specifications:

**Table 1-2. Manual Scope**

| | |
|---|---|
| Product Version | WGT624 v3 108 Mbps Wireless Firewall Router |
| Manual Publication Date | December 2005 |

**Note:** Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/WGT624 v3.asp*

## How to Use This Manual

The HTML version of this manual includes the following:

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

## How to Print this Manual

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

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

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

- **Printing a Chapter**.

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

– Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

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

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

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

• **Printing the Full Manual**.

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

– Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.

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

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

# Chapter 2
# Introduction

Congratulations on your purchase of the NETGEAR® WGT624 v3 108 Mbps Wireless Firewall Router. The WGT624 v3 wireless router provides connection for multiple computers to the Internet through an external broadband access device (such as a cable modem or DSL modem) that is normally intended for use by a single computer. This chapter describes the features of the NETGEAR WGT624 v3 108 Mbps Wireless Firewall Router.

## Key Features

The WGT624 v3 108 Mbps Wireless Firewall Router with 4-port switch connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The WGT624 v3 wireless router provides you with multiple web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, web site addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253 computers. In addition to the Network Address Translation (NAT) feature, the built-in firewall protects you from hackers.

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

The WGT624 v3 wireless router provides the following features:

- 802.11g wireless networking, with the ability to operate in 802.11g-only, 802.11-turbo-g-only, or 802.11b+g modes.
- Trend Micro Home Network Security Services to address the unique security needs of computers accessing the Internet via home routers. (Microsoft Internet Explorer V 5.5 or higher with ActiveX support is required.)
- Easy, web-based setup for installation and management.
- Content Filtering and Site Blocking Security.
- Built in 4-port 10/100 Mbps Switch.
- Ethernet connection to a wide area network (WAN) device, such as a cable modem or DSL modem.
- Extensive Protocol Support.

- Login capability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.

## 802.11g Wireless Networking

The WGT624 v3 wireless router includes an 802.11g wireless access point, providing continuous, high-speed 108 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11g wireless networking at up to 108 Mbps.
- 802.11g wireless networking, with the ability to operate in 802.11g-only, 802.11b-only, or 802.11g and b modes, providing backwards compatibility with 802.11b devices or dedicating the wireless network to the higher bandwidth 802.11g devices.
- 64-bit and 128-bit WEP (Wired Equivalent Privacy) encryption security.
- WEP keys can be generated manually or by passphrase.
- WPA-PSK and WPA2-PSK (Wi-Fi Protected Access - Pre Shared Key) support. Support for WPA data encryption which provides strong data encryption and authentication based on a pre-shared key.
- Wireless access can be restricted by MAC address.
- Wireless network name broadcast can be turned off so that only devices that have the network name (SSID) can connect.

## A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the WGT624 v3 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection.

  Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits, including Parental Controls provided by Trend Micro Home Network Security Services (Microsoft Internet Explorer V 5.5 or higher with ActiveX support is required).
- Logs security incidents.

The WGT624 v3 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to email the log to you at specified intervals. You can also configure the router to send immediate alert messages to your email address or email pager whenever a significant event occurs.

- The WGT624 v3 prevents objectionable content from reaching your computers. The router allows you to control access to Internet content by screening for keywords within web addresses. You can configure the router to log and report attempts to access objectionable Internet sites.

## Security

The WGT624 v3 wireless router is equipped with several features designed to maintain security, as described in this section.

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

## Autosensing Ethernet Connections with Auto Uplink

With its internal 4-port 10/100 switch, the WGT624 v3 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

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

## Extensive Protocol Support

The WGT624 v3 wireless router supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, see "Internet Networking and TCP/IP Addressing" in Appendix B.

- IP Address Sharing by NAT

  The WGT624 v3 wireless router allows several networked computers to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.

- Automatic Configuration of Attached Computers by DHCP

  The WGT624 v3 wireless router dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached computers on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of computers on your local network.

- DNS Proxy

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

- PPP over Ethernet (PPPoE)

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

## Easy Installation and Management

You can install, configure, and operate the WGT624 v3 108 Mbps Wireless Firewall Router within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-based management.

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

- Smart Wizard.

  The WGT624 v3 wireless router Smart Wizard automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.

- Firmware Auto-Update.

  The WGT624 v3 wireless router automatically checks the Internet to see if a newer version of firmware is available. If so, it asks you if you want to install the upgrade. This lets you take advantage of product enhancements for your WGT624 v3 as soon as they become available.

- Visual monitoring.

  The WGT624 v3 wireless router's front panel LEDs provide an easy way to monitor its status and activity.

## Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the WGT624 v3 wireless router:

- Flash memory for firmware upgrade
- Free technical support seven days a week, twenty-four hours a day

# Package Contents

The product package should contain the following items:

- WGT624 v3 108 Mbps Wireless Firewall Router.
- AC power adapter.
- Vertical stand.
- Category 5 (CAT5) Ethernet cable.
- *108 Mbps Wireless Router WGRT624 v3 Resource CD*, including:
  - — Application Notes and other helpful information.
- *108 Mbps Wireless Firewall Router WGT624 Installation Guide.*
- Registration and Warranty Card.
- Support Information Card.

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

## The Router's Front Panel

The front panel of the WGT624 v3 wireless router contains the status LEDs described below.


**Figure 2-1**

You can use some of the LEDs to verify connections. Viewed from left to right, Table 2-1 describes the LEDs on the front panel of the router. These LEDs are green when lit.

**Table 2-1. LED Descriptions**

| Label | Activity | Description |
|---|---|---|
| Power | On<br>Off | Power is supplied to the router.<br>Power is not supplied to the router. |
| Internet | On<br>Blink | The Internet (Wide Area Network) port has detected a link with an attached device.<br>Data is being transmitted or received by the Internet port. |
| Wireless | On | Indicates that the Wireless port is initialized. |
| Local | On (Green)<br>Blink (Green)<br>On (Amber)<br>Blink (Amber)<br>Off | The Local (LAN) port has detected link with a 100 Mbps device.<br>Data is being transmitted or received at 100 Mbps.<br>The Local port has detected link with a 10 Mbps device.<br>Data is being transmitted or received at 10 Mbps.<br>No link is detected on this port. |

## The Router's Rear Panel

The rear panel of the WGT624 v3 wireless router contains the port connections listed below.

**Figure 2-2**

Viewed from left to right, the rear panel contains the following features:

- AC power adapter outlet
- Four Local (LAN) 10/100 Mbps Ethernet ports for connecting the router to the local computers
- Internet (WAN) Ethernet port for connecting the router to a cable or DSL modem
- Factory Default Reset push button
- Wireless antenna

# Chapter 3
# Connecting the Router to the Internet

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

Once you are connected to the Internet and your wireless connections are working, you can also configure the router's content filtering parameters if you need to change the default settings. See Chapter 4, "Content Filtering.

If you are an advanced user, you can also configure maintenance (see Chapter 6, "Maintenance) and advanced (see Chapter 7, "Advanced Configuration) settings if you need to change the factory defaults.

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

## Initial Configuration

**1.** Insert the Resource CD into the CD drive on your computer. The following screen appears:


**Figure 3-1**

2. Click **SETUP** and follow the instructions. The Smart Wizard Installation Assistant will guide you through the setup process:
   - How to change your cabling.
   - How to connect to the Internet.
   - How to configure your wireless settings.
     - When you get to the wireless settings, you will have to select the country where you are located and decide whether you want to have security on your wireless links (Netgear strongly recommends enabling security).
     - Depending on the type of security you select, you will also have to enter security key or passphrase information (see Chapter 5, "Wireless Configuration" for information on the wireless authentication and encryption parameters).

   If you want to change your Internet or wireless settings later, see "Changing Your Configuration" on page 3-6.

3. You will get the following success page after you have finished connecting to the Internet and configuring your wireless parameters:

**Click this area to install the Trend Micro dashboard and set up your Trend Micro Account.**

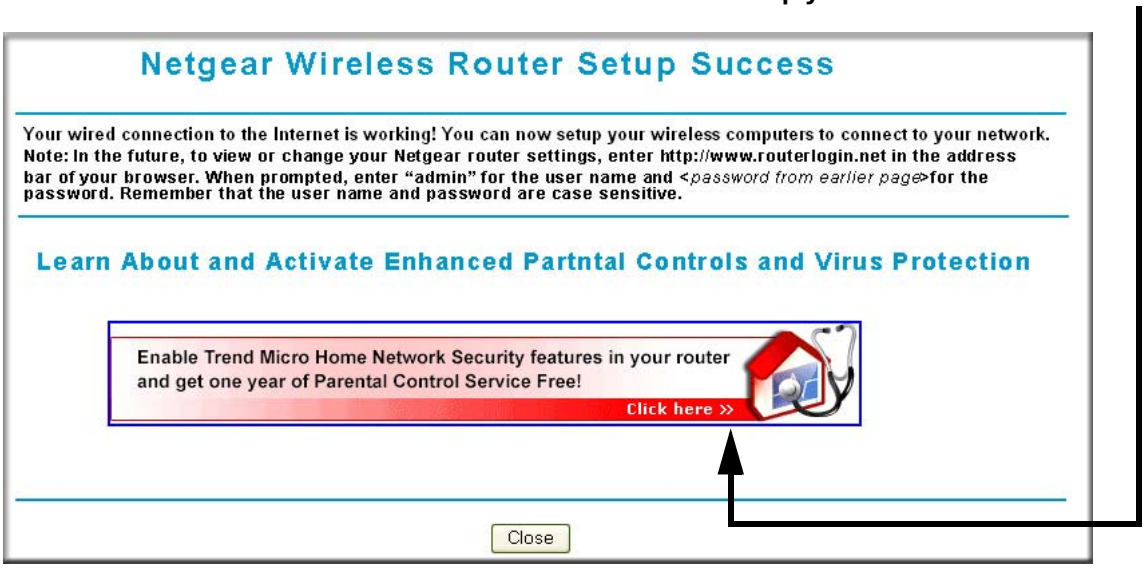



**Figure 3-2**

| | |
|---|---|
| | **Note:** The WGT624 v3 108 Mbps Wireless Firewall Router supports the Home Network Security. To take advantage of this feature, you must first establish an account with Trend Micro and your computer must support Microsoft Internet Explorer V 5.5 or higher with ActiveX support. Refer to *http://www.trendmicro.com/offers/netgear* for more information. |

Home routers provide an enhanced Internet experience, but the likelihood of attacks also increases. The Trend Micro Home Network Security Services address the unique security needs of computers accessing the Internet via home routers.

To take advantage of the Trend Micro Home Network Security Services offer, click on the Trend Micro area to go to the Trend Micro Web site to open your Trend Micro account.

| | |
|---|---|
| | **Note:** You may choose to set up the Trend Micro functions at a later time if you wish. See "Trend Micro Home Network Security" on page 4-1 for the instructions. |

# Logging Into Your Router

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

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


**Figure 3-3**

2. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters (or enter the password you chose if you changed it during the setup in "Initial Configuration" on page 3-1).

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

A login window like the one shown below opens:


**Figure 3-4**

**3.** Click **OK** and the resulting window below appears:


**Figure 3-5**

4. Enable the Firmware Upgrade Assistant if you want the router to check for the lastest firmware every time you log into the router (otherwise, you can check yourself manually; see "Upgrading the Router Software" on page 6-4).

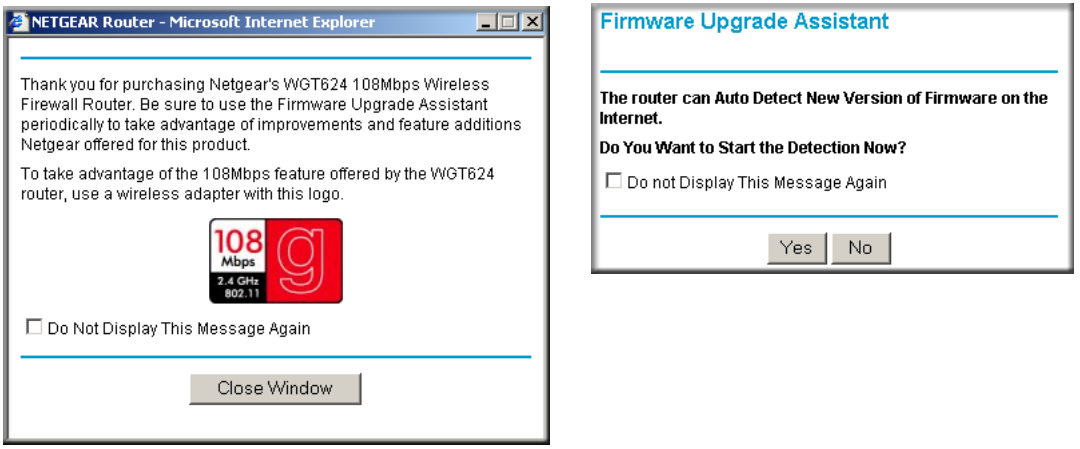



**Figure 3-6**

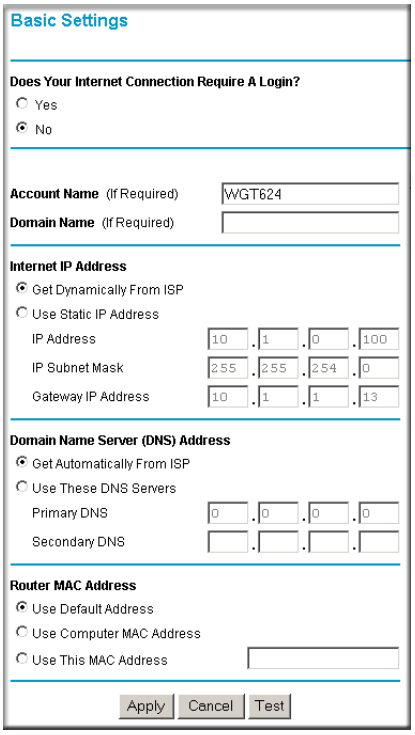
# Changing Your Configuration

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

## Internet Settings

To change the Internet settings, click **Basic Settings** on the left menu bar. One of the following screens appears:

**Basic Settings, No Login**




**Basic Settings, Login Required**

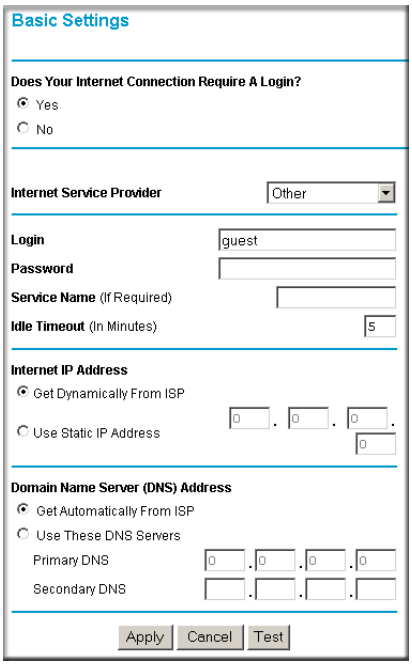



**Figure 3-7**

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.

For the most current documentation, go to:
*http://kbserver.netgear.com/products_automatic/WGT624v3.asp*

| | |
|---|---|
| | **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 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 box.

  Some ISPs (like Mindspring, Earthlink, and T-DSL) require that you use your full e-mail address when you log in. If your ISP requires your full e-mail address, then type it in the Login box.

  – **Password**: Type the password that you use to log in to your ISP.

  – **Service Name**: If your ISP provided a Service Name, enter it here. Otherwise, this may be left blank.

  – **Idle Timeout**: An idle Internet connection will be terminated after this time period.

  If this value is zero (0), then the connection will be "kept alive" by re-connecting immediately whenever the connection is lost.

- **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 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 put JerAB in this box.

  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 into the correct boxes.

  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 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 Web site, it is likely that your DNS servers aren't set up properly. You should contact your ISP to get DNS server addresses.

- **Router MAC Address**: Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address.

  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.

Click **Test** to connect to the NETGEAR Web site. If you connect successfully, your settings work and you may click **Logout** to exit these pages and... enjoy surfing the 'net!

If you don't connect successfully,

1. Go through the settings and make sure you've selected the correct options and typed everything correctly.
2. Contact your ISP to verify the configuration information.
3. Read the Troubleshooting section in the Router Installation Guide.
4. On the Router GearBox CD, read the Troubleshooting Guide or the Troubleshooting section in the Reference Manual.
5. Contact NETGEAR Technical Support.

## Using the Smart Setup Wizard

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

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

1. Connect to the wireless router by typing **http://www.routerlogin.net** in the address field of your browser, then click **Enter**.
2. For security reasons, the router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 6-7.

   **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 v3 wireless router and display the home page as shown in Figure 3-5 on page 3-5.
3. Click **Setup Wizard** on the upper left of the main menu.
4. Click **Next** to proceed. Input your ISP settings, as needed.
5. At the end of the Setup Wizard, click the **Test** button to verify your Internet connection. If you have trouble connecting to the Internet, see Chapter 8, "Troubleshooting".

# NETGEAR Product Registration, Support, and Documentation

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

Product updates and Web support are always available by going to:
*http://kbserver.netgear.com/products/WGT624v3.asp*

Documentation is available on the CD and at
*http://kbserver.netgear.com/documentation/WGT624.asp*

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

# Chapter 4
# Content Filtering

This chapter describes how to use the content filtering features of the WGT624 v3 108 Mbps Wireless Firewall Router to protect your network. These features can be found by under the Content Filtering heading in the main menu of the browser interface.

The WGT624 v3 108 Mbps Wireless Firewall Router provides you with web content filtering options, plus browser activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted-access policies based on time-of-day, web addresses and web address keywords. You can also block Internet access by applications and services, such as chat or games.

## Trend Micro Home Network Security

You can enable the Home Network Security here if you did not do so when you originally set up your WGT624 v3 wireless router (see "Initial Configuration" on page 3-1).

**Note:** The WGT624 v3 108 Mbps Wireless Firewall Router supports the Home Network Security. To take advantage of this feature, you must first establish an account with Trend Micro and your computer must support Microsoft Internet Explorer V 5.5 or higher with ActiveX support. Refer to *http://www.trendmicro.com/offers/netgear* for more information.

Home routers provide an enhanced Internet experience, but the likelihood of attacks also increases. The Trend Micro Home Network Security Services address the unique security needs of computers accessing the Internet via home routers.

Once you have established your Trend Micro account, you must enable and program the Service Settings and Parental Controls menus on your WGT624 v3 wireless router to be able to use the Home Network Security with the WGT624 v3 wireless router:

Each screen has a GUI button to click that will take you to the Trend Micro Web site to open your Trend Micro account.

## Service Settings

Click **Security Service** under Content Filtering on the main menu to display the Service Settings menu shown below:

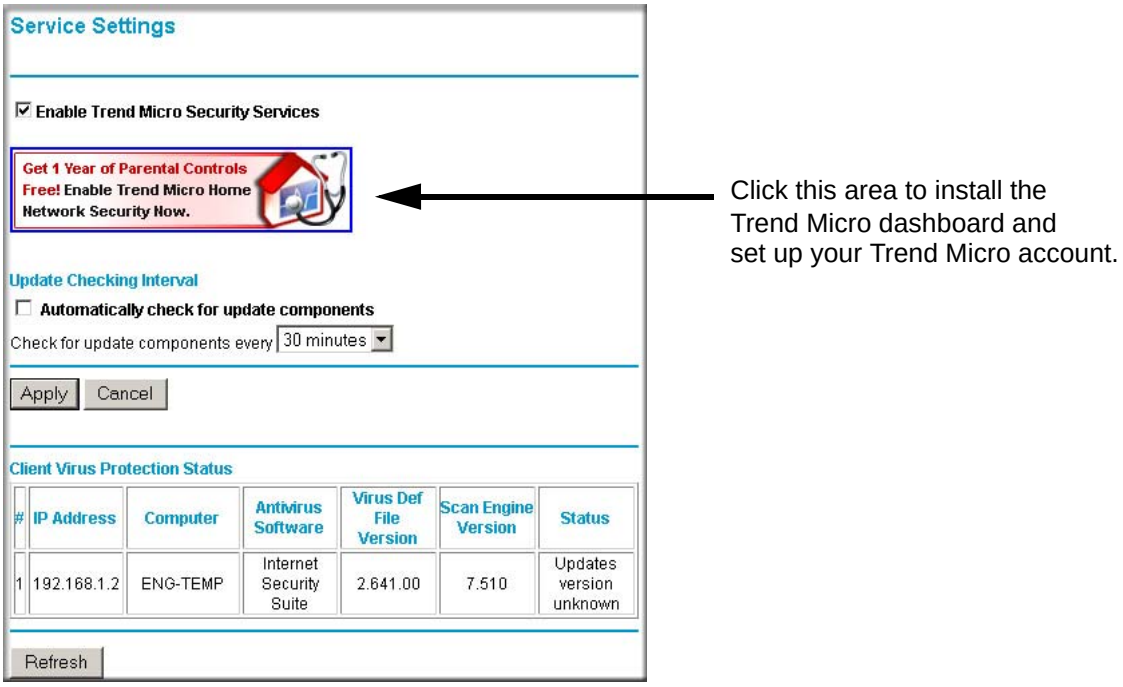



**Figure 4-1**

- **Enable Trend Micro Security Services**: Check or clear this checkbox to enable or disable the Trend Micro Security Services.
- C**heck for update of Trend Micro Internet Security:** choose when to automatically check the Trend Micro ActiveUpdate server for updated components. Options include:
  - 10 minutes
  - 20 minutes
  - 30 minutes
  - 1 hour
  - 2 hours
  - 3 hours
  - 1 day

| | |
|---|---|
|  | **Note:** If your ISP bills by the amount of time or traffic you use, you might want to set this update frequency to once a day |

- **Client Virus Protection Status:** provides information on all computers on the network including whether the computer has installed antivirus software and the status of the update components.
  - **IP Address**: The computer IP address
  - **Computer Name**: The name of the computer
  - **Antivirus Software**: The type of virus protection software installed on the computer
  - **Virus Definition File Version**: The version of the virus pattern file in use by the virus protection software
  - **Scan Engine**: The version of the scan engine in use by the virus protection software
  - **Status**: This status is based on how current the update components (virus definition file, scan engine) are in use

## Parental Controls

| | |
|---|---|
|  | **Note:** A particular Web site can be blocked by either Netgear keyword blocking (see "Blocking Access to Internet Sites" on page 4-8) or Home Network Security parental controls. A Netgear trusted IP address will be overridden by Home Network Security parental controls. |

Click **Parental Controls** under Content Filtering on the main menu to display the Parental Controls menu shown below:

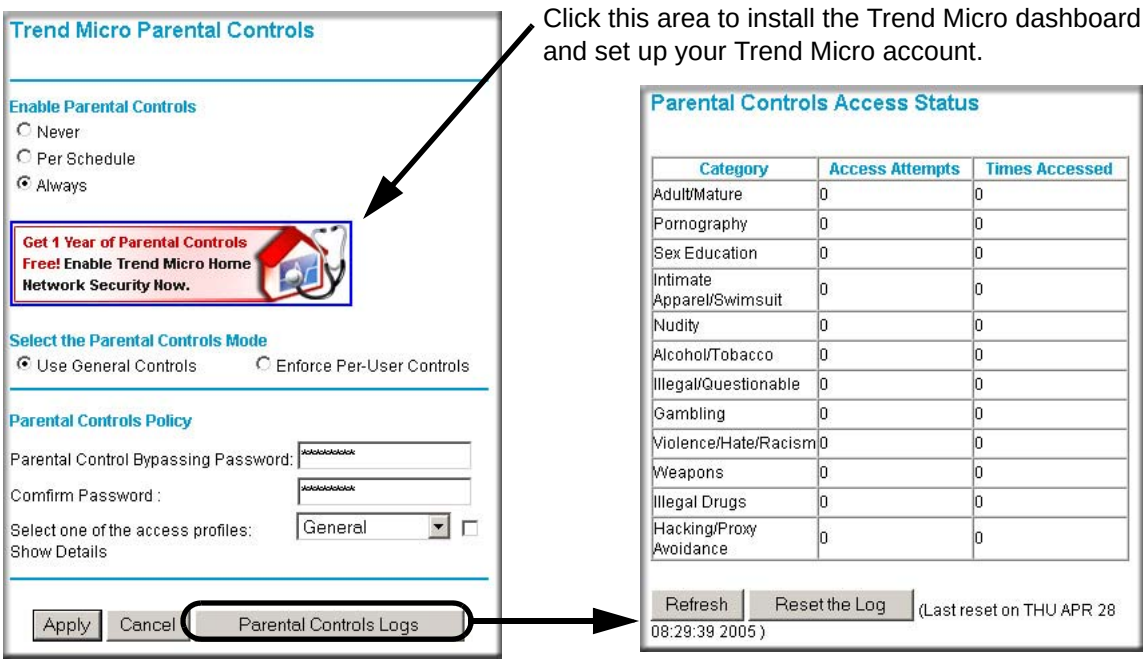



**Figure 4-2**

To enable Parental Controls, choose one of the following options:

- Click **Per Schedule** to turn on Parental Controls and block according to the settings on the Schedule page.
- Click **Always** to turn on Parental Controls to allow blocking all of the time, independent of the Schedule page.

| | |
|---|---|
| | **Note:** On the Schedule page you can set when keyword, domain name and Parental Controls blocking occurs. |

To disable Parental Controls, click **Never**.

To select Parental Controls Mode, choose one of the following:

- Select the **Use General Controls** radio button to create a blanket setting that allows access to Web sites that contain content that are appropriate for viewing by all users accessing the Internet through the router.
- Select the **Enforce Per-User Controls** radio button to allow access to certain categories of Web sites on a per-user basis.

> **Note:** When in Per-User mode, everyone accessing the Internet through the router is required to log in.

- Parental Controls Bypassing Password (General mode): Enter a password into the Parental Controls Bypassing Password box. Then enter the password a second time in the Confirm Password box to confirm that both passwords match. With this password, users can view Web sites containing content that would normally be blocked by the Parental Controls setting
- Parental Controls User Account (Per-User only): The User List lists the names of the users currently accessing the Internet, the level of access they have (as determined by Parental Controls Setting), and whether they are enabled in the system or not.

> **Note:** Users on the user list cannot log in or access the Internet if “Enforce Per-Use Controls” is not enabled.

**a.** Click **Add User** to give permission to a user to access the internet through the router.

> **Note:** When in Per-User mode, everyone accessing the Internet through the router will have to log in.

**b.** Under the Account Information section, enter a name for the person wanting access to the Internet.

**c.** Then enter a password that the user will be required to use when attempting to access the internet.

**d.** Enter the password again in the Confirm Password textbox.

**e.** Finally, next to the Status section, choose whether to enable or disable this person’s account.

- Parental Controls Access Profile: The Parental Controls Policy is the same for both Per-User and General mode. The Parental Controls Policy has five predefined blocking categories and one custom category. The categories are:
  - General
  - PG13
  - Young Adult
  - No Restrictions
  - Custom

  By default, the General category is selected, this blocks all of the 12 categories listed under the Potentially Offensive heading. (Note: When manually selecting the categories from the Potentially Offensive section, the Custom menu item will automatically be selected)
- Parental Controls Categories: Choose which categories of Web sites to block.Options include:
  - **Adult/Mature Content**: Sites that contain material of an adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These sites include very profane or vulgar content and sites that are not appropriate for children.
  - **Alcohol/Tobacco**: Sites that promote or offer for the sale alcohol/tobacco products, or provide the means to create them. Also includes sites that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. Does not include sites that sell alcohol or tobacco as a subset of other products.
  - **Gambling**: Sites where a user can place a bet or participate in a betting pool (including lotteries) online. Also includes sites that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. Does not include sites that sell gambling related products or machines. Also does not include sites for offline casinos and hotels (as long as those sites do not meet one of the above requirements).
  - **Hacking/Proxy Avoidance**: Sites providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server.
  - **Illegal Drugs**: Sites that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
  - **Illegal/Questionable**: Sites that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. Also includes sites that provide or sell questionable educational materials, such as term papers.

- **Intimate Apparel/Swimsuit**: Sites that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. Does not include sites selling undergarments as a subsection of other products offered.
- **Nudity Sites**: containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include sites containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist sites that contain pictures of nude individuals.
- **Pornography**: Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
- **Sex Education**: Sites that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. Also includes sites that offer tips for better sex as well as products used for sexual enhancement.
- **Violence/Hate/Racism**: Sites that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. Also includes sites that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics.
- **Weapons**: Sites that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. Does not include sites that promote collecting weapons, or groups that either support or oppose weapons use.

**Note:** Parental Controls Policy defaults to the General rating which blocks all of the above categories. By manually selecting the above categories, the Custom menu will be selected.

# Blocking Access to Internet Sites

The WGT624 v3 wireless router allows you to restrict access based on web addresses and web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is below:

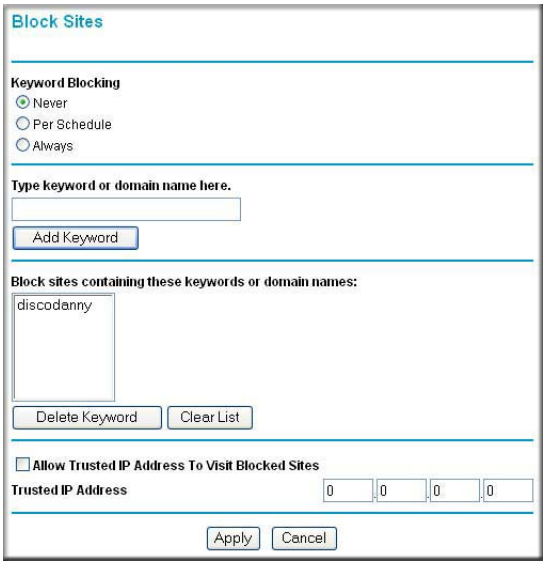



**Figure 4-3**

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

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

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

Keyword application examples:

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

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

**Note:** A particular Web site can be blocked by either Netgear keyword blocking or Home Network Security parental controls (see "Parental Controls" on page 4-3). A Netgear trusted IP address will be overridden by Home Network Security parental controls.

## Blocking Access to Internet Services

The WGT624 v3 wireless router allows you to block the use of certain Internet services by computers on your network. This is called services blocking or port filtering. The Block Services menu is shown below:

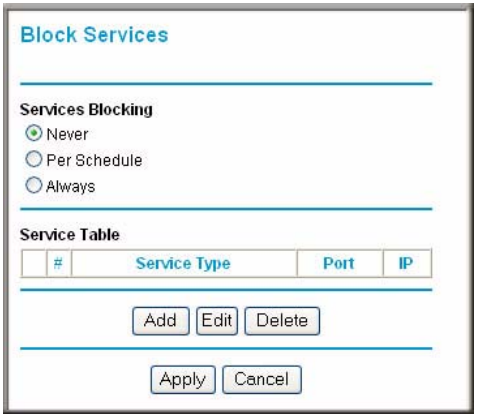



**Figure 4-4**

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

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

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

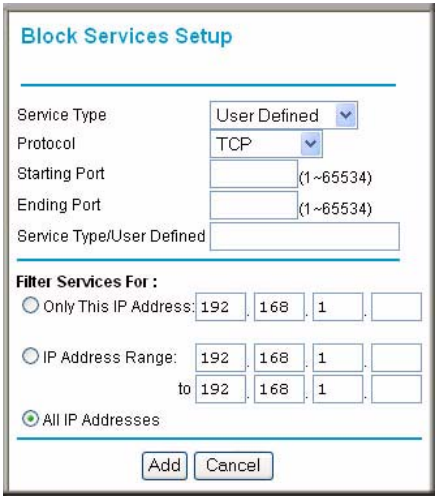



**Figure 4-5**

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

## Configuring a User Defined Service

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

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

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

## Configuring Services Blocking by IP Address Range

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

# Scheduling When Blocking Will Be Enforced

The WGT624 v3 wireless router allows you to specify when blocking will be enforced. The Schedule menu is shown below:

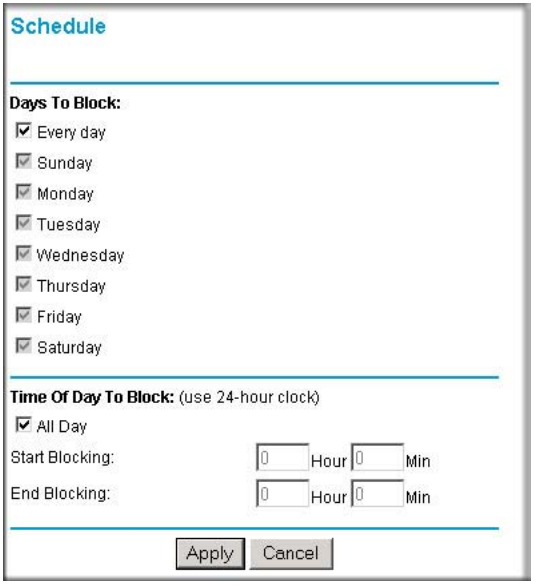



**Figure 4-6**

Use the check boxes on this menu to create a schedule for blocking content:

1. Days to Block. Select days to block by checking the appropriate boxes. Select **Every Day** to check the boxes for all days..
2. Time of Day to Block. Select a start and end time in 24-hour format. Select **All Day** for 24 hour blocking.
3. Click **Apply**.
4. Select your time zone in the E-Mail menu. For details, see the following section, “Configuring E-Mail Alert and Web Access Log Notifications”.

# Configuring E-Mail Alert and Web Access Log Notifications

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

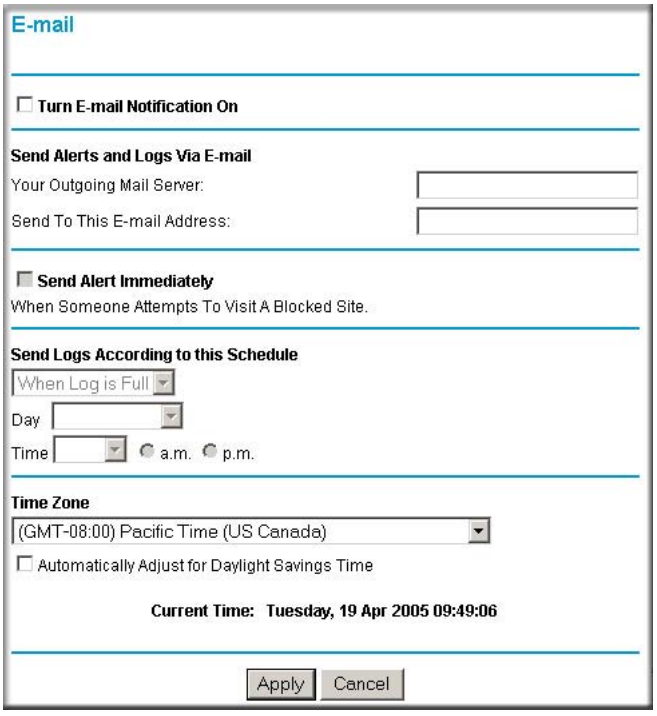



**Figure 4-7**

- Turn E-mail Notification On.

  Check this box if you wish to receive e-mail logs and alerts from the router.

- Your Outgoing Mail Server.

  Enter the name of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.

- Send To This E-mail Address.

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

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

- Send Alert Immediately.

  Check this box if you would like immediate notification of attempted access to a blocked site.

- Send Logs According to this Schedule.

  Specifies how often to send the logs: None, Hourly, Daily, Weekly, or When Full.

  – Day for sending log. Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.

  – Time for sending log. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents. If you don't want logs sent, select **None** from the list in the Send Logs According To This Schedule area. When you turn on e-mail notification and choose None in the Send Logs According to this Schedule list, the alert is sent but not the log.

The WGT624 v3 wireless router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your time zone:

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

Click **Apply** to save your settings.

# Viewing Logs of Web Access or Attempted Web Access

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

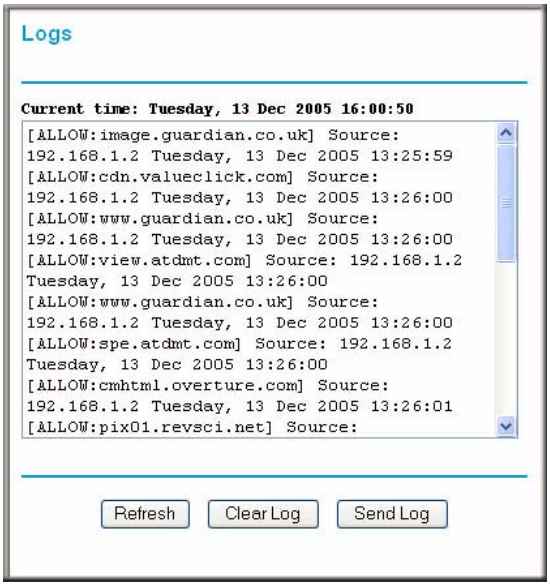



**Figure 4-8**

Log entries are described in Table 4-1

**Table 4-1. 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 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. |

Log action buttons are described in Table 4-2

**Table 4-2. 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 5
# Wireless Configuration

This chapter describes how to configure the wireless features of your WGT624 v3 wireless router. In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your wireless router in order to maximize the network speed. For further information on wireless networking, see in "Wireless Communications" in Appendix B.

## Observing Performance, Placement, and Range Guidelines

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

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

For best results, place your wireless router:

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

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP (Wired Equivalent Privacy) connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

# Implementing Appropriate Wireless Security

**Note:** Indoors, computers can connect over 802.11b/g wireless networks at ranges of up to 500 feet. Such distances can allow for others outside of your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WGT624 v3 wireless router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

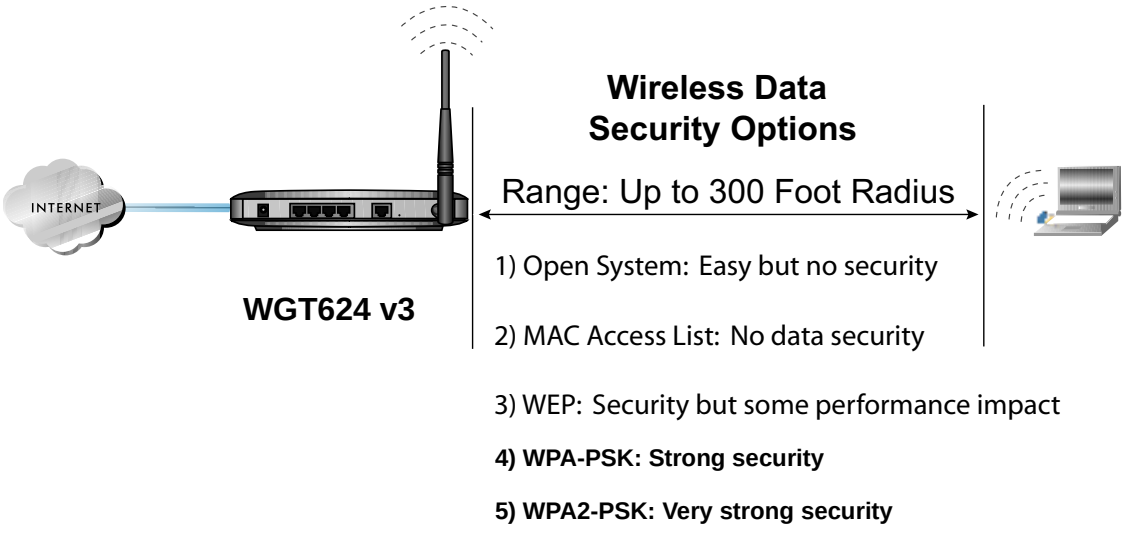



**Figure 5-1**

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 o that unknown computers cannot wirelessly connect to the WGT624 v3. 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.

## Understanding Wireless Settings

To configure the Wireless settings of your wireless router, click the **Wireless Settings** link in the Setup section of the main menu. The Wireless Settings menu will appear in one of three forms, depending on your security settings, as shown below.

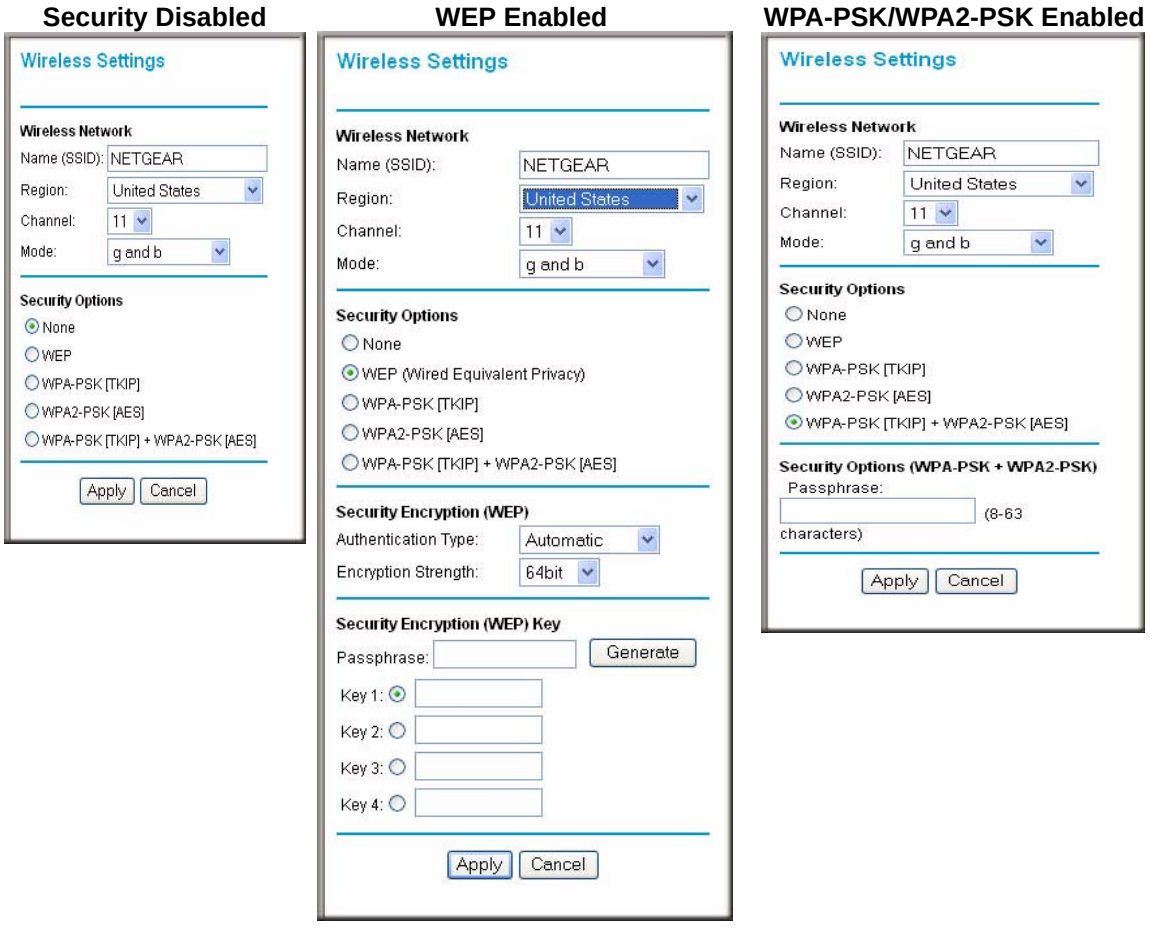



**Figure 5-2**

The 802.11b and 802.11g wireless networking protocols are configured in exactly the same fashion.

- **Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network will need to use this SSID for that network. The WGT624 v3 default SSID is: **NETGEAR**.

- **Region.** This field identifies the region where the WGT624 v3 can be used. It may not be legal to operate the wireless features of the wireless router in a region other than one of those identified in this field.
- **Channel.** This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point. For a link to more information on the wireless channel frequencies, see "Wireless Communications" in Appendix B.
- **Mode.** This field determines which data communications protocol will be used. You can select "Auto 108 Mbps", "g only", or "g and b". The "g only" option dedicates the WGT624 v3 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.** These options are the wireless security features you can enable. The table that follows identifies the various basic wireless security options. For a link to a full explanation of these standards, see "Wireless Communications" in Appendix B.

| Field | Description |
|---|---|
| **Automatic** | No wireless security. |
| **WEP** | WEP offers the following options:<br>• Open System<br>With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the WGT624 v3 *does* perform 64- or 128-bit data encryption but *does not* perform any authentication.<br>• Shared Key<br>Shared Key authentication encrypts the SSID and data.<br>Choose the Encryption Strength (64- or 128-bit data encryption). Manually enter the key values or enter a word or group of printable characters in the Passphrase box. Manually entered keys *are* case sensitive but passphrase characters *are not* case sensitive.<br>**Note**: Not all wireless adapter configuration utilities support passphrase key generation.<br>• Auto<br>The wireless router automatically detects whether Open System or Shared Key is used. |
| **WPA-PSK**<br>**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.<br>Enter a word or group of printable characters in the Passphrase box. These characters *are* case sensitive.<br>**Note**: Not all wireless adapter configuration utilities support WPA. Furthermore, client software is required on the client. Windows XP Service Pack 2 and Windows XP Service Pack 1 with the WPA patch do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. |

**Note:** If you do not see the “WPA2-PSK [AES]” and “WPA-PSK [TKIP] + WPA2-PSK[AES]” options on your Wireless Settings menu, you need to update the router software. See “Upgrading the Router Software” on page 6-4 for details.

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

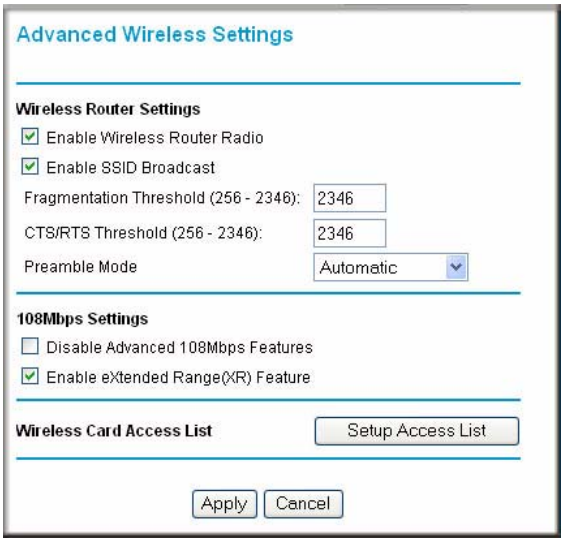



**Figure 5-3**

- **Enable Wireless Router Radio.** If you disable the wireless router radio, wireless devices cannot connect to the WGT624 v3.
- **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.
- **Wireless Card Access List.** When the Trusted PCs Only radio button is selected, the WGT624 v3 checks the MAC address of the wireless station and only allows connections to computers identified on the trusted computers list.
- **108Mbps Settings.**
  - **Disable Advanced 108Mbps Features**: disables data compression, packet bursting, and large frame support.
  - **Enable eXtended Range**: provides singnificantly 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. |

## Information to Gather Before Changing the Wireless Settings

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

- **Wireless Network Name (SSID)*:*** _____ The SSID identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID *is* case sensitive. The SSID in the wireless adapter card must match the SSID of the wireless router. In some configuration utilities (such as in Windows XP), the term "wireless network name" is used instead of SSID.
- **If WEP Authentication is Used,** circle one: **Open System**, **Shared Key, or Auto**.

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

  - **WEP Encryption key size**. Choose one: **64-bit** or **128-bit**. Again, the encryption key size must be the same for the wireless adapters and the wireless router.
  - **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.
    - **Passphrase method**. _____ These characters *are* case sensitive. Enter a word or group of printable characters and click **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. When you use WPA-PSK, the other devices in the network will not connect unless they are set to WPA-PSK as well and are configured with the correct Passphrase. Similarly, when you use WPA2-PSK, the other devices in the network will not connect unless they are aslo set to WPA2-PSK and are configured with the correct Passphrase.

Use the procedures described in the following sections to configure the WGT624 v3. Store this information in a safe place.

## Default Factory Settings

When you first receive your WGT624 v3, the default factory settings are shown below. You can restore these defaults with the Factory Default Restore button on the rear panel. After you install the WGT624 v3 wireless router, use the procedures below to customize any of the settings to better meet your networking needs.

| FEATURE | DEFAULT FACTORY SETTINGS |
|---|---|
| Wireless Access Point | **Enabled** |
| Wireless Access List (MAC Filtering) | **All wireless stations allowed** |
| SSID broadcast | **Enabled** |
| SSID | **NETGEAR** |
| 11b/g RF Channel | **11** |
| Mode | **g and b** |
| Authentication Type | **Open System** |
| WEP | **Disabled** |

## How to Set Up and Test Basic Wireless Connectivity

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

1. Log in to the WGT624 v3 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 main menu of the WGT624 v3 wireless router.


**Figure 5-4**

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

> **Note:** The 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.

4. Set the region. Select the region in which the wireless interface will operate.
5. If necessary, set the channel. The default channel is 11.

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. 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.

6. For initial configuration and test, leave or set "Security Options" to **Disable**.
7. Click **Apply** to save your changes.

**Warning:** If you are configuring the router from a wireless computer and you change the router's SSID, channel, or security settings, you will lose your wireless connection when you click **Apply**. You must then change the wireless settings of your computer to match the firewall's new settings. For this reason, it is best to use a wired connection between the computer and the router while changing the basic setup or security settings.

8. Configure and test your computers for wireless connectivity.

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

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

## How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the WGT624 v3 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. From the Security Options section, select **WEP (Wired Equivalent Privacy)**. The WEP options display.

**4.** Select the Authentication Type and Encryption Strength from the drop-down lists.


**Figure 5-5**

Normally “Authentication Type” can be left at the default value of “Automatic”. If that fails, select the appropriate value “Open System” or “Shared Key”. Check your wireless card's documentation to see what method to use.

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

5. From the Security Encryption menu drop-down list, select the WEP encryption strength you will use.

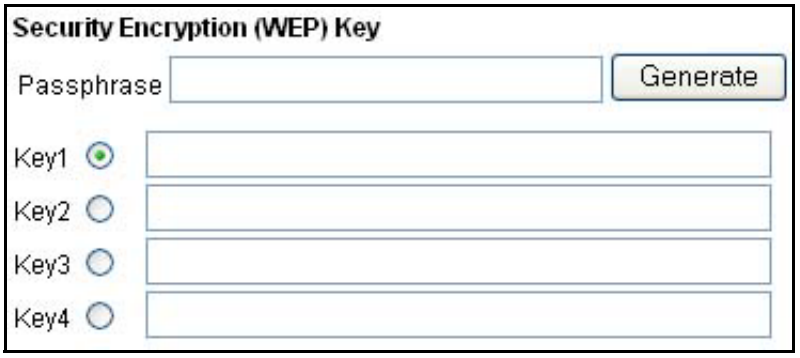



**Figure 5-6**

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.
   - Automatic—enter a word or group of printable characters in the Passphrase box and 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.

| | |
|---|---|
|  | **Warning:** If you are configuring the router from a wireless computer and you change the router's SSID, channel, or security settings, you will lose your wireless connection when you click **Apply**. You must then change the wireless settings of your computer to match the firewall's new settings. For this reason, it is best to use a wired connection between the computer and the router while changing the security settings. |

# How to Configure WPA-PSK/WPA2-PSK Wireless Security

**Note:** Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP and Windows 2000 with Service Pack 3 do include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless computers or PDAs (Personal Digital Assistants) for WPA-PSK security, consult the documentation for the product you are using.

To configure WPA-PSK, follow these steps:

1. Click **Wireless Settings** in the Setup section of the main menu and select the **WPA-PSK [TKIP]**, **WPA2-PSK [AES]**, or **WPA-PSK [TKIP] + WPA2-PSK [AES]** option for the Security Type. The WPA-PSK [TKIP] + WPA2-PSK[AES] option is recommended, since that option is compatible with a greater number of devices.

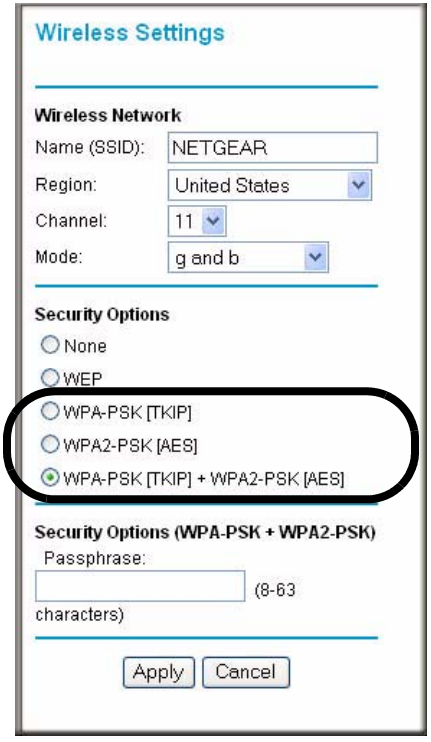



**Figure 5-7**

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

## How to Restrict Wireless Access by MAC Address

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

1. Log in to the WGT624 v3 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 menu, click **Setup Access List** to display the Wireless Card Access Setup menu shown below.

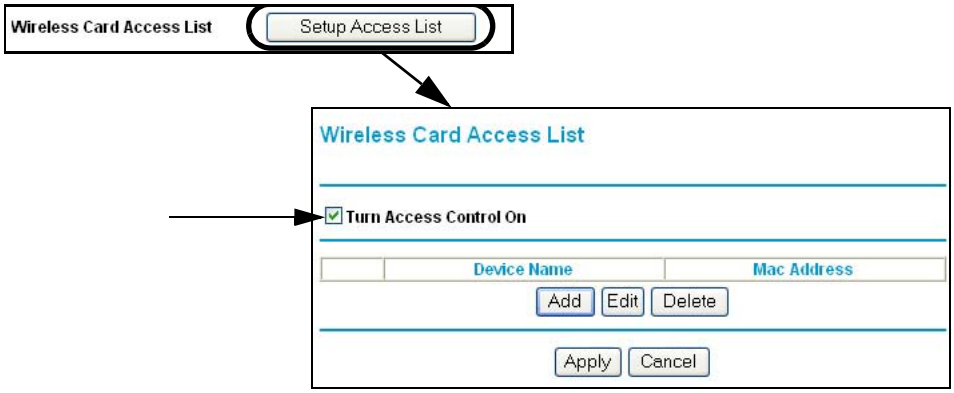



**Figure 5-8**

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.

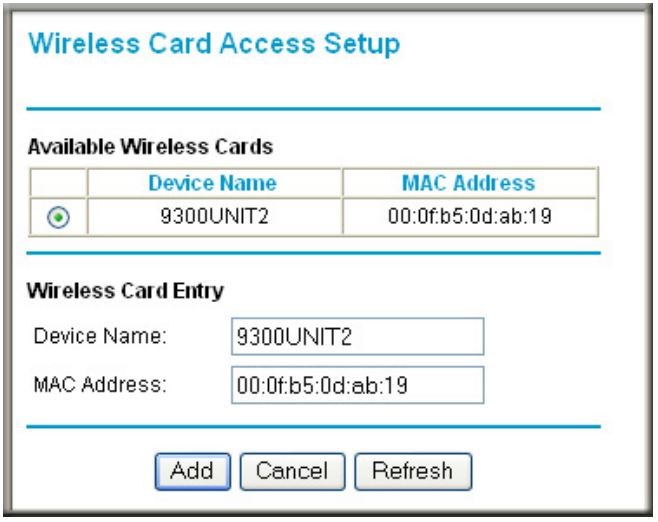



**Figure 5-9**

6. In the Available Wireless Cards list, either select from the list of cards the WGT624 v3 has found in your area, or enter the MAC address and device name for a device you plan to use. You can usually find the MAC address printed on the wireless adapter.

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

7. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen. 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 v3.

# Chapter 6
# Maintenance

This chapter describes how to use the maintenance features of your WGT624 v3 108 Mbps Wireless Firewall Router. These features can be found under the Maintenance heading in the main menu of the browser interface.

## Viewing Wireless Router Status Information

The Router Status menu provides a limited amount of status and usage information. From Maintenance section of the main menu, select **Router Status** to view the Router Status screen, shown below.

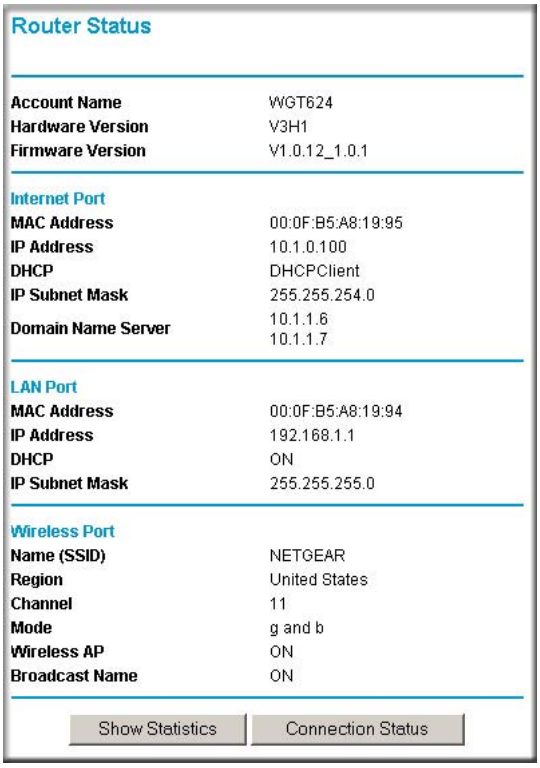



**Figure 6-1**

This screen shows the following parameters:

**Table 6-1. Menu 3.2 - Wireless Router Status Fields**

| Field | Description |
|---|---|
| Account Name | This field displays the Host Name assigned to the router. |
| Firmware Version | This field displays the router firmware version. |
| Internet Port | These parameters apply to the Internet (WAN) port of the router. |
| MAC Address | This field displays the Media Access Control address being used by the Internet (WAN) port of the router. |
| IP Address | This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet. |

**Table 6-1. Menu 3.2 - Wireless Router Status Fields (continued)**

| Field | Description |
|---|---|
| DHCP | If set to None, the router is configured to use a fixed IP address on the WAN.<br>If set to Client, the router is configured to obtain an IP address dynamically from the ISP. |
| IP Subnet Mask | This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router. |
| Domain Name Server | Displays the address of the current Domain Name Server |
| LAN Port | These parameters apply to the Local (WAN) port of the router. |
| MAC Address | This field displays the Media Access Control address being used by the LAN port of the router. |
| IP Address | This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.1.1. |
| DHCP | Identifies if the router's built-in DHCP server is active for the LAN attached devices. |
| IP Subnet Mask | This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0 |
| Wireless Port | These parameters apply to the Wireless port of the router. |
| Name (SSID) | This field displays the wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR. |
| Region | This field displays the geographic region where the router being used. It may be illegal to use the wireless features of the router in some parts of the world. |
| Channel | Identifies if the channel the wireless port is using. See "Wireless Communications" in Appendix B for a link to a document that details the frequencies used on each channel. |
| Mode | Indicates the current mode (g & b, g only, b only, or Auto 108 Mbps) |
| Wireless AP | Indicates if the Access Point feature of the router is enabled. If not enabled, wireless devices will not be able to connect to the network. |
| Broadcast Name | Indicates if the wireless router is broadcasting its SSID. |

## Viewing a List of Attached Devices

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

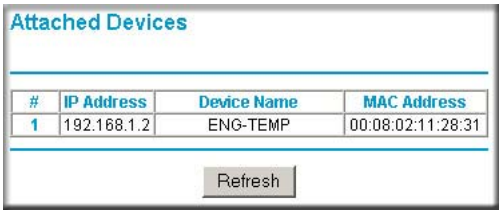



**Figure 6-2**

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 Software

The router software of the WGT624 v3 wireless router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

**Note:** The web browser used to upload new firmware into the WGT624 v3 wireless router must support HTTP uploads. Use Microsoft Internet Explorer or Netscape Navigator 4.0 or above. Do not interrupt the upgrade process once it has started.

**Note:** Be sure to check the NETGEAR web site for documentation updates which are available at *http://www.netgear.com/docs*.

From the Maintenance section of the main menu, select the **Router Upgrade** heading to display the menu shown below.


**Figure 6-3**

**Note:** When uploading software to the WGT624 v3 wireless router, it is important not to interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your router will automatically restart. The upgrade process will typically take about one minute.

To check for new firmware, click **Check**.If the WGT624 v3 finds new firmware is available, follow the on-screen prompts to download in install the new firmware.

To upload firmware from your hard drive:

1. In the Router Upgrade menu, click **Browse** and browse to the location of the binary (.chk) upgrade file.
2. Click **Upload**.

**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 WGT624 v3 wireless router are stored within the router in a configuration file. This file can be saved (backed up) to a user's computer, retrieved (restored) from the user's computer, or cleared to factory default settings.

From the Maintenance section of the main menu, click the **Backup Settings** link to display the menu shown below.

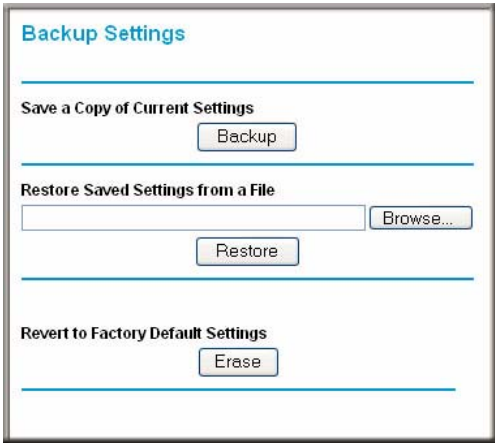



**Figure 6-4**

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

## Backing Up and Restoring the Configuration

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

To save your settings, click **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

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

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

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

# Changing the Administrator Password

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

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


**Figure 6-5**

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

# Chapter 7
# Advanced Configuration

This chapter describes how to configure the advanced features of your WGT624 v3 108 Mbps Wireless Firewall Router. These features can be found under the Advanced heading in the main menu of the browser interface.

## Configuring Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make a local server (for example, a web server or game server) visible and available to the Internet. This is done using the Port Forwarding menu. From the Advanced section of the main menu, click **Port Forwarding / Port Triggering** to view the port forwarding menu, shown below.

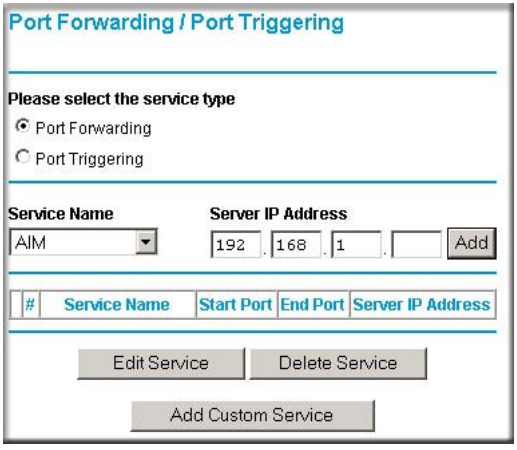



**Figure 7-1**

| | |
|---|---|
| | **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. |

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

## Editing or Deleting a Port Forwarding Entry

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

1. In the table, select the button next to the service name.
2. Click **Edit 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. The assigned IP address can be found in the Maintenance Status Menu, where it is shown as the WAN IP Address.

Some considerations for this application are:

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

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

Some online games and videoconferencing applications are incompatible with NAT. The WGT624 v3 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 is an advanced feature that 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:

- A computer makes an outgoing connection using a port number defined in the Port Triggering table.
- This 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.
- The remote system receives the computer's request, and responds using a different port number.
- This 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 this 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.

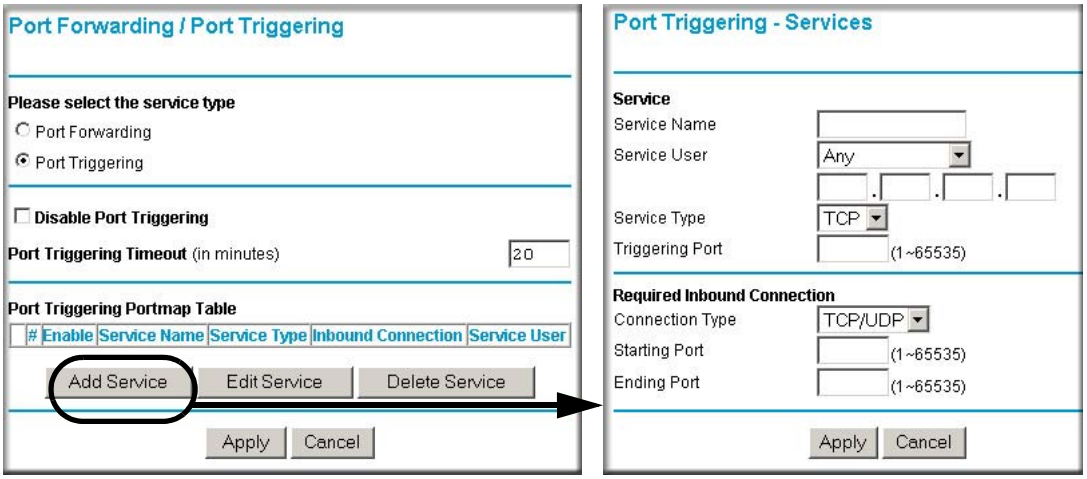



**Figure 7-2**

### Adding a new Service

To add a new service, click **Add Service** and enter the following data on the resulting screen.

**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 the service to be used by everyone on the network. 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

   The inbound connection information can be obtained from the game or applications manual or the product’s support Web site.

### Editing or Deleting a Service

To edit an existing service:

1. From the Port Triggering menu, 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 above, and click **Apply.**

# Configuring WAN Setup Options

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

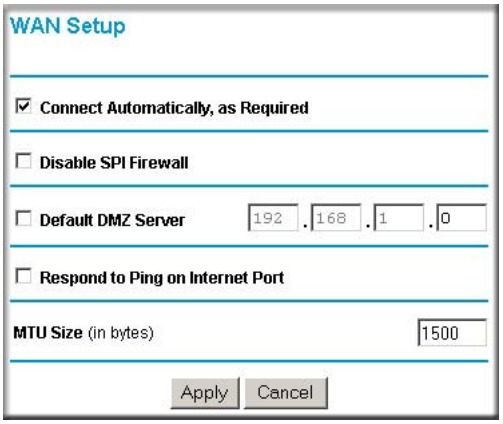



**Figure 7-3**

- Connect Automatically, as Required.

  Normally, this option should be enabled. An Internet connection will be made automatically after each timeout, whenever Internet-bound traffic is detected. This provides connection on demand and is potentially cost-saving.

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

- 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 WGT624 v3. 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.

- Setting Up a Default DMZ Server.

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

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

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

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

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

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

## Respond to a Ping on the Internet WAN Port

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

## Setting the MTU Size

The default MTU size does not usually need to be changed. The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, particularly some using PPPoE, you may need to reduce the MTU. This should not be done 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 which 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 main menu of the browser interface, under Advanced, click **Dynamic DNS**.

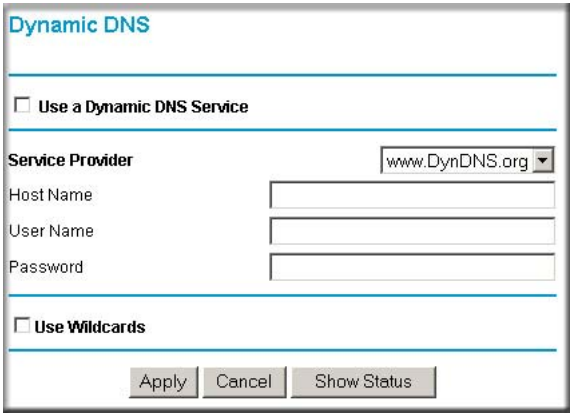



**Figure 7-4**

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

# Using LAN IP Setup Options

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

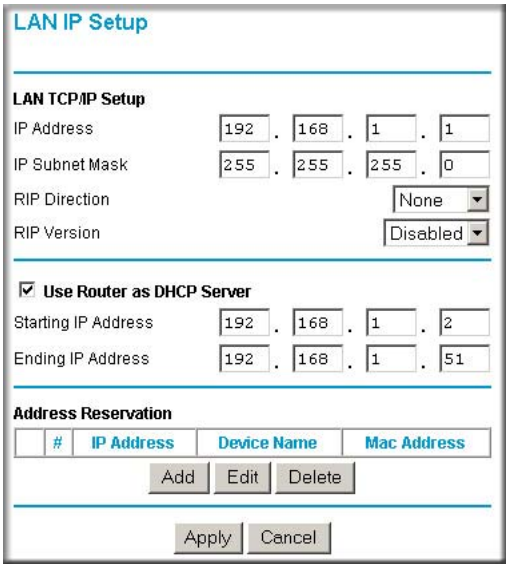



**Figure 7-5**

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.

  — When set to Both or Out Only, the router will broadcast its routing table periodically.

  — When set to Both or In Only, it will incorporate the RIP information that it receives.

  — When set to None (default), it will not send any RIP packets and will ignore any RIP packets received.

- RIP Version.

  This controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, 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 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 checked.

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

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

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

## Using Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer will always receive the same IP address each time it 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. From the LAN IP Setup screen, click **Add**.

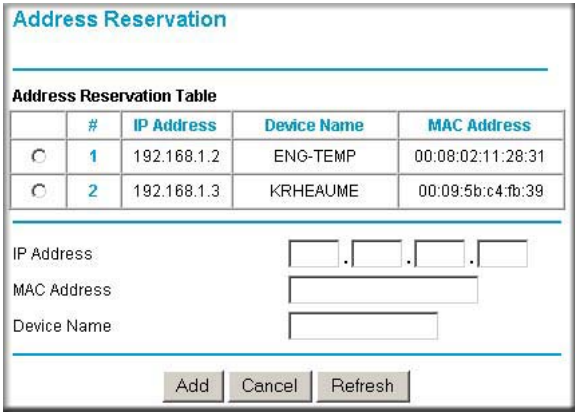



**Figure 7-6**

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 menu and paste it here. See "Viewing a List of Attached Devices" on page 6-4

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.

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


**Figure 7-7**

To add or edit a Static Route:

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

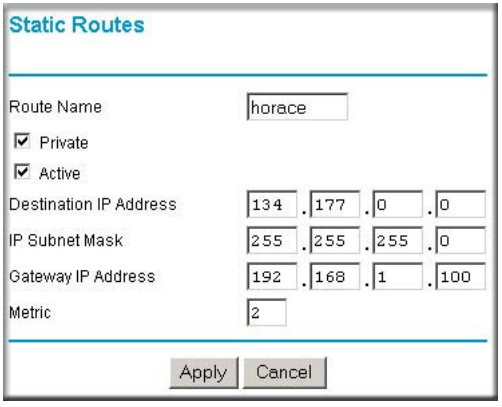



**Figure 7-8**

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

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

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

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

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.1.100. The static route would look like Figure 7-8.

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 specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.1.100.
- A Metric value of 1 will work since the ISDN router is on the LAN.

- Private is selected only as a precautionary security measure in case RIP is activated.

## Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your WGT624 v3 wireless router.

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

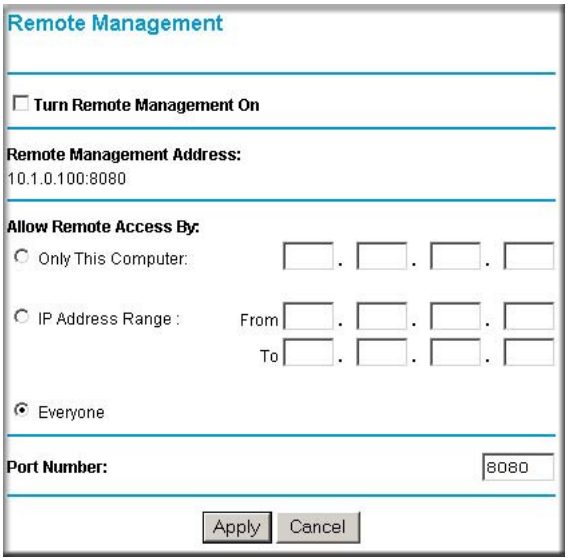



**Figure 7-9**

To configure your router for Remote Management:

1. Select the **Turn Remote Management On** check box.
2. 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 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 PC**. Enter the IP address that will be allowed access.

**3.** 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.

**4.** 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.

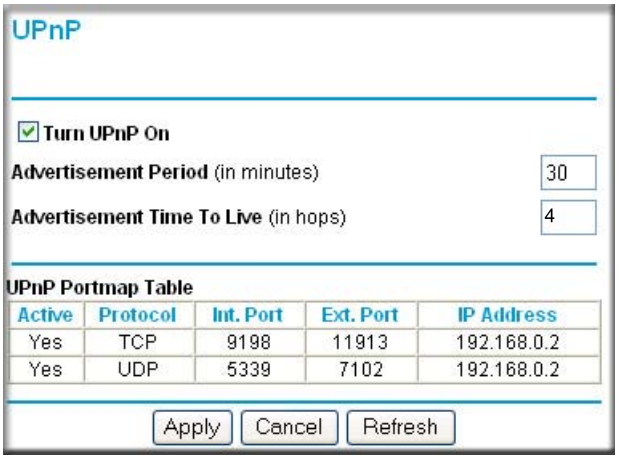



**Figure 7-10**

**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 8
# Troubleshooting

This chapter gives information about troubleshooting your WGT624 v3 108 Mbps Wireless Firewall Router. After each problem description, instructions are provided to help you diagnose and solve the problem.

**Note:** Product updates are available on the NETGEAR Web site at *www.netgear.com/support/main.asp*.

## 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. (**Note**: The LED is off in factory default setting and is enabled/LIT after you run the Configuration Assistant.)

   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 turns 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 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 8-7.

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.

# Troubleshooting the Web Configuration Interface

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

- Check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.1.2 to 192.168.1.254. See "Preparing a Computer for Network Access" on page B-1 for a link to a document that describes how to find your computr'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 auto-generated 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 8-7.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

- When entering configuration settings, be sure to click **Apply** before moving to another menu or tab, 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 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 menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:

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

OR

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

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

- Your computer may not recognize any DNS server addresses.

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

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

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

# Troubleshooting a TCP/IP Network Using a Ping Utility

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

## Testing the LAN Path to Your Router

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

To ping the router from a 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 8-2.
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
  - — Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

## Testing the Path from Your Computer to a Remote Device

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

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

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

If the path is functioning correctly, replies 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 as described in "Preparing a Computer for Network Access" in Appendix B.
- — Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- — Check that your cable or DSL modem is connected and functioning.
- — If your ISP assigned a host name to your computer, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single computer connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized computer.

## Restoring the Default Configuration and Password

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

- Use the Erase function of the router (see "Erasing the Configuration" on page 6-7).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

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

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

## Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The WGT624 v3 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 check the date and time again.
- Time is off by one hour. Cause: The router does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked "Adjust for Daylight Savings Time".

# Appendix A
# Technical Specifications

This appendix provides technical specifications for the WGT624 v3 108 Mbps Wireless Firewall Router.

| | |
|---|---|
| **Network Protocol and Standards Compatibility** | |
| Data and Routing Protocols: | TCP/IP, RIP-1, RIP-2, DHCP<br>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<br>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)<br>2.412~2.484 GHz (Japan)<br>2.412~2.472 GHz (Europe ETSI) |
| Encryption: | 40-bit (also called 64-bit), 128-bit WEP data encryption |

# Appendix B
# Related Documents

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

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