Reference Manual for the Double 108 Mbps Wireless Firewall Router WGU624

NETGEAR

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

M-10153-01
Version 1.1
September 2004

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.

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

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

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

FCC Caution

1. FCC RF Radiation Exposure Statement: The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

Europe - EU Declaration of Conformity

CE 0560 !	This device is a 2.4/5.0 GHz dual band low power RF device intended for home and office use in EU and EFTA member states. In some EU / EFTA member states some restrictions may apply. Please contact local spectrum management authorities for further details before putting this device into operation.

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

EN 300 328, EN 301 489-17, EN 60950-1 Safety of Information Technology Equipment, Including Electrical Business Equipment EN 300 328 V1.4.1 (2003-04) Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission system; data transmission equipment operating in the 2.4 Ghz ISM band and using spread spectrum modulation techniques; Part 1: Technical characteristics and test conditions; Part 2; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.

EN 301 489-1, Aug. 2002; EN 301 489-17, Aug. 2002 - Electromagnetic compatibility and radio spectrum matters (ERM); electromagnetic compatibility (EMC); standard for radio equipment and services: Part 1: Common technical requirements; Part 17: Specific conditions for Wideband Data and Hiperlan equipment.

EN 55 022 Declaration of Conformance

This is to certify that the Double 108 Mbps Wireless Firewall Router WGU624 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).

Compliance with the applicable regulations is dependent upon the use of shielded cables. It is the responsibility of the user to procure the appropriate cables.

Requirements For Operation in the European Community

Countries of Operation and Conditions of Use in the European Community

The user should run the configuration utility program provided with this product to check the current channel of operation and confirm that the device is operating in conformance with the spectrum usage rules for European Community countries as described in this section. European standards dictate a maximum radiated transmit power of 100mW EIRP and a frequency range of 2.400 - 2.4835 Ghz.

Operation Using 2.4 GHz Channels in France

The following radio channel usage limitations apply in France.

The radio spectrum regulator in France, Autorité de regulation des telecommunications (ART), enforces the following rules with respect to use of 2.4GHz spectrum in various locations in France. Please check ART's Web site for latest

requirements for use of the 2.4GHz band in France: http://www.art-telecom.fr/eng/index.htm. When operating in France, this device may be operated under the following conditions:

Indoors only, using any channel in the 2.4465-2.4835 GHz band.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das Double 108 Mbps Wireless Firewall Router WGU624 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 Double 108 Mbps Wireless Firewall Router WGU624 has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

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

Voluntary Control Council for Interference (VCCI) Statement

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

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

Read instructions for correct handling.

Customer Support

Refer to the Support Information Card that shipped with your Double 108 Mbps Wireless Firewall Router WGU624.

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.

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, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the Netgear website.

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

italics	Emphasis, books, CDs, URL names
bold	User input
`courier font`	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.

This manual is written for the WGU624 wireless router according to these specifications.:

Table 1-2. Manual Scope

Product Version	Double 108 Mbps Wireless Firewall Router WGU624
Manual Publication Date	September 2004

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/WGU624.asp*.

How to Use This Manual

The HTML version of this manual includes a variety of navigation features as well as links to PDF versions of the full manual and individual chapters.

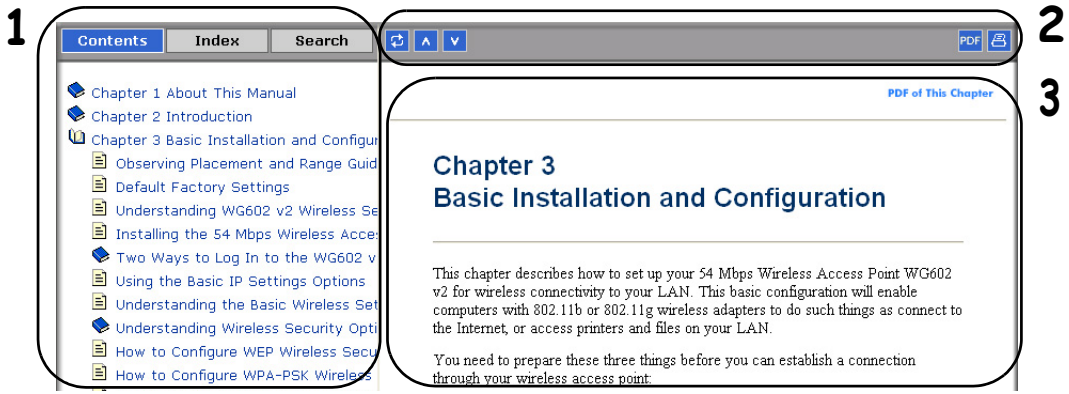


Figure 1 -1: HTML version of this manual

1. **Left pane**. Use the left pane to view the Contents, Index, Search, and Favorites tabs.

   To view the HTML version of the manual, you must have a version 4 or later browser with JavaScript enabled.

2. **Toolbar buttons**. Use the toolbar buttons across the top to navigate, print pages, and more.

   
   The Show in Contents button locates the current topic in the Contents tab.

   
   Previous/Next buttons display the previous or next topic.

   The PDF button links to a PDF version of the full manual.

   
   The Print button prints the current topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer--you do not have to worry about specifying the correct range of pages.

3. **Right pane**. Use the right pane to view the contents of the manual. Also, each page of the manual includes a PDF of This Chapter link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

How to Print this Manual

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

- **Printing a "How To" Sequence of Steps in the HTML View**. Use the *Print* button  on the upper right of the toolbar to print the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer--you do not have to worry about specifying the correct range of pages.
- **Printing a Chapter**. Use the PDF of This Chapter link at the top right of any page.
  - Click "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 save paper an printer ink by selecting this feature.
- **Printing the Full Manual**. Use the PDF button in the toolbar at the top right of the browser window.
  - Click the PDF button  on the upper right of the toolbar. The PDF version of the chapter you were viewing opens in a browser window.
  - Click the print icon in the upper left of the window.

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

Chapter 2
Introduction

Congratulations on your purchase of the NETGEAR® Double 108 Mbps Wireless Firewall Router WGU624. The WGU624 wireless router provides connection for multiple personal computers (PCs) 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 PC. This chapter describes the features of the NETGEAR Double 108 Mbps Wireless Firewall Router WGU624.

Key Features of the Router

The Double 108 Mbps Wireless Firewall Router WGU624 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 WGU624 wireless router provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts — both 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 personal 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 WGU624 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.
- 802.11a wireless networking
- Channel bonding combines the bandwidth of two radio channels into one communications link (54 Mbps +54 Mbps =108 Mbps) between the router and wireless stations
- Super A and Super G modes
- Easy, Web-based setup for installation and management.
- Content Filtering and Site Blocking Security.

- Built-in 4-port 10/100 Mbps Switch.
- LAN port 4 is a built-in hardware DMZ port
- Ethernet connection to a wide area network (WAN) device, such as a cable modem or DSL modem.
- Extensive protocol support.
- Login capability
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrades.

802.11 a/g Wireless Networking

The WGU624 wireless router includes 802.11 a and 802.11g wireless access points, providing continuous, high-speed access between your wireless and Ethernet devices. The router provides:

- 802.11g and 802.11a wireless networking at up to 108 Mbps.
- 802.11g wireless networking, with the ability to operate in 802.11g-only, 802.11-turbo-g-only, or 802.11b+g modes, providing backwards compatibility with 802.11b devices or dedicating the wireless network to the higher bandwidth 802.11g devices.
- 802.11a wireless networking, with the ability to operate in 802.11a-only, 108 Mbps only, or Auto 108 Mbps modes.
- When Super G Modes is enabled, the wireless router will enable channel bonding, data compression, packet bursting and large frame support. Channel bonding takes two of the three usable channels in 2.4GHz 802.11b/g and uses them to double the speed.
- 64-, 128-, and 152-bit WEP encryption security.
- WEP keys can be generated manually or by passphrase.
- WPA and WPA-PSK wireless security.
- 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.

Comparing the 802.11a, 802.11b, and 802.11g Modes

The Double 108 Mbps Wireless Firewall Router WGU624 offers a variety of wireless modes. The table below compares some of the features of each mode.

Table 2-1. Comparison of Wireless Modes

Features	802.11b	802.11a	Super A	802.11g	Super G
Performance	11 Mbps	54 Mbps	108 Mbps	54 Mbps	108 Mbps
Range	In practice, about 100 feet indoors. Up to 1500 feet in the open.	Less than “b”	More than “a”	Two times “b”	Four times “b”
Compatibility	802.11b only	Only with normal 802.11a	802.11a	802.11g and 802.11b (Can use a “g” router with a “b” adapter.)	802.11g and 802.11b
Channel	Any	Any	Any	Any	6
Frequency	2.4 GHz	5 GHz	5 GHz	2.4 GHz	2.4 GHz

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the WGU624 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection.

  Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.

- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents.

  The WGU624 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to e-mail the log to you at specified intervals. You can also configure the router to send immediate alert messages to your e-mail address or e-mail pager whenever a significant event occurs.

- The WGU624 prevents objectionable content from reaching your PCs. 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 WGU624 wireless router is equipped with several features designed to maintain security, as described in this section.

- PCs 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 PCs on the LAN.
- DMZ Hardware Port
  A Demilitarized Zone (DMZ) is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network.

  The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.
- Port Forwarding with NAT
  Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the router allows you to direct incoming traffic to specific PCs 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 8-port 10/100 switch, the WGU624 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 automatically senses whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a PC or an ‘uplink’ connection such as to a switch or hub. That port then configures itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

Extensive Protocol Support

The WGU624 wireless router supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to Appendix B, “Network, Routing, Firewall, and Basics”.

- IP Address Sharing by NAT
  The WGU624 wireless router allows several networked PCs 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 PCs by DHCP
  The WGU624 wireless router dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs 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 PCs. 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 PC.

Easy Installation and Management

You can install, configure, and operate the Double 108 Mbps Wireless Firewall Router WGU624 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 WGU624 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 WGU624 wireless router automatically checks the Internet to see if a newer version of firmware is available. If so, it asks if you want to install the upgrade. This lets you take advantage of product enhancements for your WGU624 as soon as they become available.
- Visual monitoring
  The WGU624 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 WGU624 wireless router:

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

Package Contents

The product package should contain the following items:

- Double 108 Mbps Wireless Firewall Router WGU624.
- AC power adapter.
- Vertical stand.
- Category 5 (CAT5) Ethernet cable.
- *Double 108 Mbps Wireless Router WGU624 Resource CD* , including:
  - The *Setup Manual for the WGU624*.
  - Application Notes and other helpful information.
- *Installation Guide for the WGU624.*
- 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 WGU624 wireless router contains the status LEDs described below.

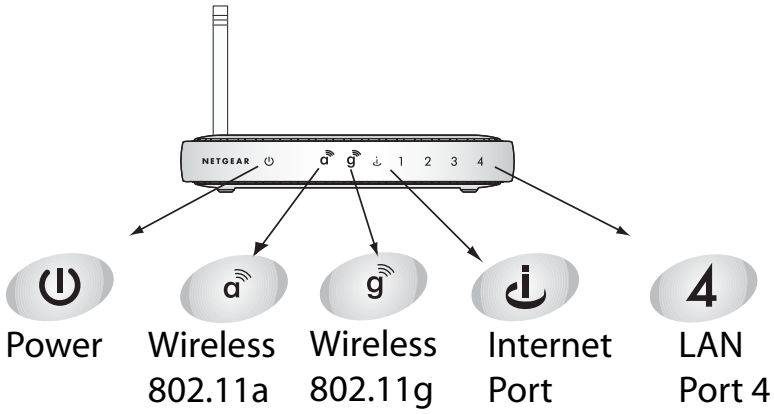


Figure 2-1: WGU624 Front Panel

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

Table 2-1. LED Descriptions

Label	Activity	Description
Power	On Amber Blink Off	Power is supplied to the router. Power is supplied to the router and it is performing its diagnostic test. Power is not supplied to the router.
802.11a	On	The 802.11a wireless interface is enabled.
802.11g	On	The 802.11g wireless interface is enabled.

Table 2-1. LED Descriptions

Internet	On Blink	The Internet (WAN) port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
4 Local	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The Local (LAN) port has detected link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected on this port.

The Router's Rear Panel

The rear panel of the WGU624 wireless router contains the port connections listed below.

Figure 1-2: WGU624 Rear Panel

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

- AC power adapter outlet
- Four Local (LAN) 10/100 Mbps Ethernet ports, the fourth can be used with a DMZ server
- 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 set up the router on your local area network (LAN) and connect to the Internet. You will find out how to configure your Double 108 Mbps Wireless Firewall Router WGU624 for Internet access using the Setup Wizard, or how to manually configure your Internet connection.

What You Will Need Before You Begin

You need to prepare these three things before you begin:

1. Have active Internet service such as that provided by an cable or DSL broadband account.
2. Locate the Internet Service Provider (ISP) configuration information for your DSL account.
3. Network capability to connect the router to a cable or DSL modem and a computer as explained below.

Cabling and Computer Hardware Requirements

To use the WGU624 wireless router on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (Cat 5) cable such as the one provided with your router. The cable or DSL broadband modem must provide a standard 10 Mbps (10BASE-T) or 100 Mbps (10BASE-Tx) Ethernet interface.

Computer Network Configuration Requirements

The WGU624 includes a built-in Web Configuration Manager. To access the configuration menus on the WGU624, your must use a Java-enabled Web browser program that supports HTTP uploads such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer or Netscape Navigator 4.0 or above.

For the initial setup of your router, you need to connect a computer to the router. This computer has to be set to automatically get its TCP/IP configuration from the router via DHCP.

Note: For help with DHCP configuration, please use the Windows TCP/IP Configuration Tutorials on the *Double 108 Mbps Wireless Router WGU624 Resource CD* , or refer to Appendix C, "Preparing Your Network".

Internet Configuration Requirements

Depending on how your ISP set up your Internet account, you will need one or more of these configuration parameters to connect your router to the Internet:

- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses
- Fixed IP Address which is also known as Static IP Address

Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information.

- Your ISP provides all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
  - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
  - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
  - For Macintosh computers, open the TCP/IP or Network control panel. Record all the settings for each section.
- You may also refer to the *Double 108 Mbps Wireless Router WGU624 Resource CD* for the NETGEAR Router ISP Guide, which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below.

Record Your Internet Connection Information

Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

ISP Login Name: The login name and password are case sensitive and must be entered exactly as given by your ISP. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you connect using a login name and password, then fill in the following:

Login Name: _____

Password: _____

Service Name: _____

Fixed or Static IP Address: If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: _____ _____ _____ _____

Gateway IP Address: _____ _____ _____ _____

Subnet Mask: _____ _____ _____ _____

ISP DNS Server Addresses: If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: _____ _____ _____ _____

Secondary DNS Server IP Address: _____ _____ _____ _____

Host and Domain Names: Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you haven't been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is **aaa@yyy.com**, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _____ ISP Domain Name: _____

For Wireless Access: For configuration of the wireless network, record the following:
Wireless Network Name (SSID): _____

Encryption (circle one): WEP 64, or WEP 128

WEP passphrase or key: _____

Connecting the WGU624

This section provides instructions for connecting the Double 108 Mbps Wireless Firewall Router WGU624. Also, the *Double 108 Mbps Wireless Router WGU624 Resource CD* included with your router contains an animated Installation Assistant to help you through this procedure.

Connecting the Wireless Router

Follow the steps below to connect your router to your network. You can also refer to the *Double 108 Mbps Wireless Router WGU624 Resource CD* included with your router which contains an animated Installation Assistant to help you through this procedure.

1. **CONNECT THE WIRELESS ROUTER, THE COMPUTER, AND THE MODEM.**

   a. Turn off your computer and your cable or DSL modem.

   b. Locate the Ethernet cable (Cable 1 in the diagram below) that connects your PC to the modem.

   c. Disconnect the cable at the computer end only, point **A** in the diagram.

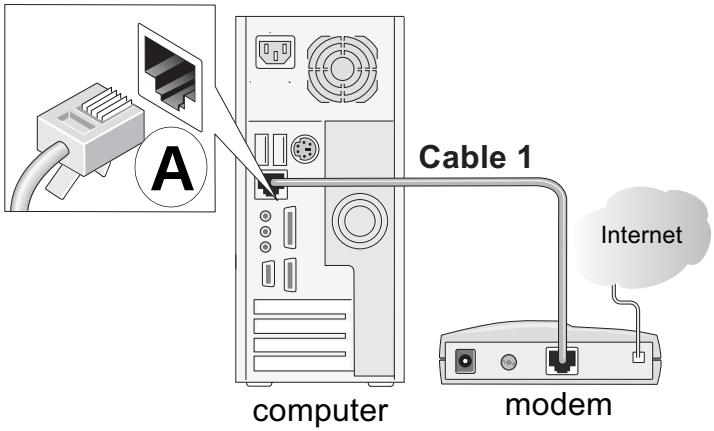


Figure 3-1: Disconnect the Ethernet cable from the computer

   d. Look at the label on the bottom of the wireless router. Locate the Internet port. Securely insert the Ethernet cable from your modem (Cable 1 in the diagram below) into the Internet port of the wireless router as shown in point **B** in the diagram below.

Note: Place the WGU624 wireless router in a location which conforms to the "Observing Performance, Placement, and Range Guidelines" on page 4-1. The stand provided with the WGU624 provides a convenient, space-saving way of installing the wireless router. Avoid stacking it on other electronic equipment.

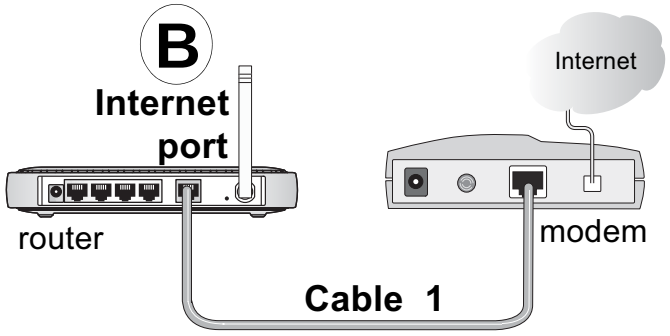


Figure 3-2: Connect the wireless router to the modem

e. Securely insert the blue cable that came with your wireless router into a LAN port on the router such as LAN port 4 (point C in the diagram), and the other end into the Ethernet port of your computer (point D in the diagram).

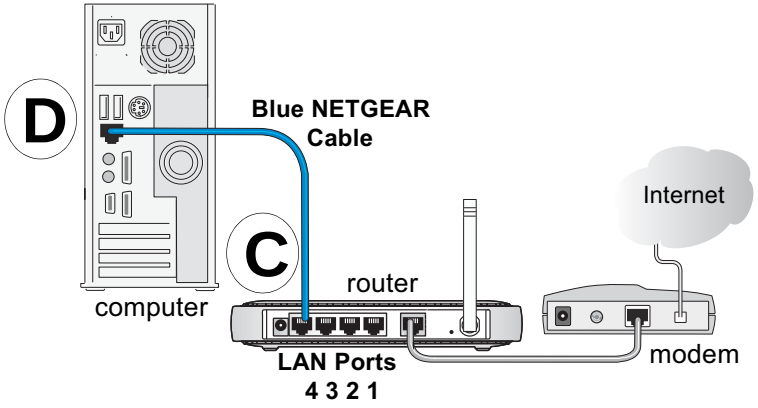


Figure 3-3: Connect the computers on your network to the router

Your network cables are connected and you are ready to restart your network.

2. Restart Your Network in the Correct Sequence

Warning: Failure to restart your network in the correct sequence could prevent you from connecting to the Internet.

a. First, turn on the broadband modem and wait 2 minutes.

b. Now, plug in the power cord to the WGU624 and wait one minute.

c. Last, turn on your computer.

Note: For DSL customers, if software logs you in to the Internet do not run that software. You may need to go to the Internet Explorer Tools Menu, Internet Options, Connections tab page where you can select "Never dial a connection".

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

When you turn the router on, the power light goes on.

The Wireless a and g lights should be lit.

The router's local LAN lights 4 are lit for any computers that are connected to it.

The router's Internet light is lit, indicating a link has been established to the cable or DSL modem.

Note: For wireless placement and range guidelines, and wireless configuration instructions, please see Chapter 4, "Wireless Configuration".

3. Open a Browser and Log In to the Wireless Router.

Note: To connect to the router, your computer needs to be configured to obtain an IP address automatically via DHCP. If you need instructions on how to do this, please refer to Appendix C, "Preparing Your Network".

a. Connect to the router by typing *http://192.168.1.1* in the address field of Internet Explorer or Netscape® Navigator.

b. 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.

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.

The login window is displayed below:

Figure 3-4: Login window

c. Click OK.

Note: If you cannot connect to the wireless router, verify that your cables are connected correctly, that the router is powered on. Verify that your computer is set to obtain the *both* IP and DSN server addresses automatically, which is usually so. For help with this, see the tutorials on the *Resource CD*.

4. CONNECT TO THE INTERNET

Figure 3-5: Setup Smart Wizard

a. You are now connected to the router. If you do not see the menu above, click the Setup Smart Wizard link on the upper left of the main menu.

b. Click Next and follow the steps in the Setup Smart Wizard for inputting the configuration parameters from your ISP to connect to the Internet.

   Note: If you choose not to use the Setup Smart Wizard, you can manually configure your Internet connection settings by following the procedure "How to Manually Configure Your Internet Connection" on page 3-9.
   Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP that you recorded in the form, "Record Your Internet Connection Information" on page 3-3.

c. When the router successfully detects an active Internet service, the router's Internet LED goes on. The Setup Smart Wizard reports which connection type it discovered, and displays the appropriate configuration menu. If the Setup Smart Wizard finds no connection, you will be prompted to check the physical connection between your router and the cable or DSL line.

d. The Setup Smart Wizard will report the type of connection it finds and prompts you for the settings. The options are:

   - Connections that require a login using protocols such as PPTP, Telstra Bigpond, or PPPoE or Other broadband connections.
   - Connections that use dynamic IP address assignment.
   - Connections that use fixed IP address assignment.

e. When the router successfully detects an active Internet service, the router checks to see of there is a new version of firmware available. If so, you will be prompted to upgrade your firmware. Take advantage of this opportunity to assure that your wireless router is up to date with the latest enhancements and features.

   If you choose not to use the auto-update feature, you can check for new firmware by following the procedure in "Upgrading the Router Software" on page 6-5.

Note: Be sure to check the NETGEAR Web site for documentation updates, which are available at *http://kbserver.netgear.com/products/WGU624.asp*.

How to Manually Configure Your Internet Connection

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

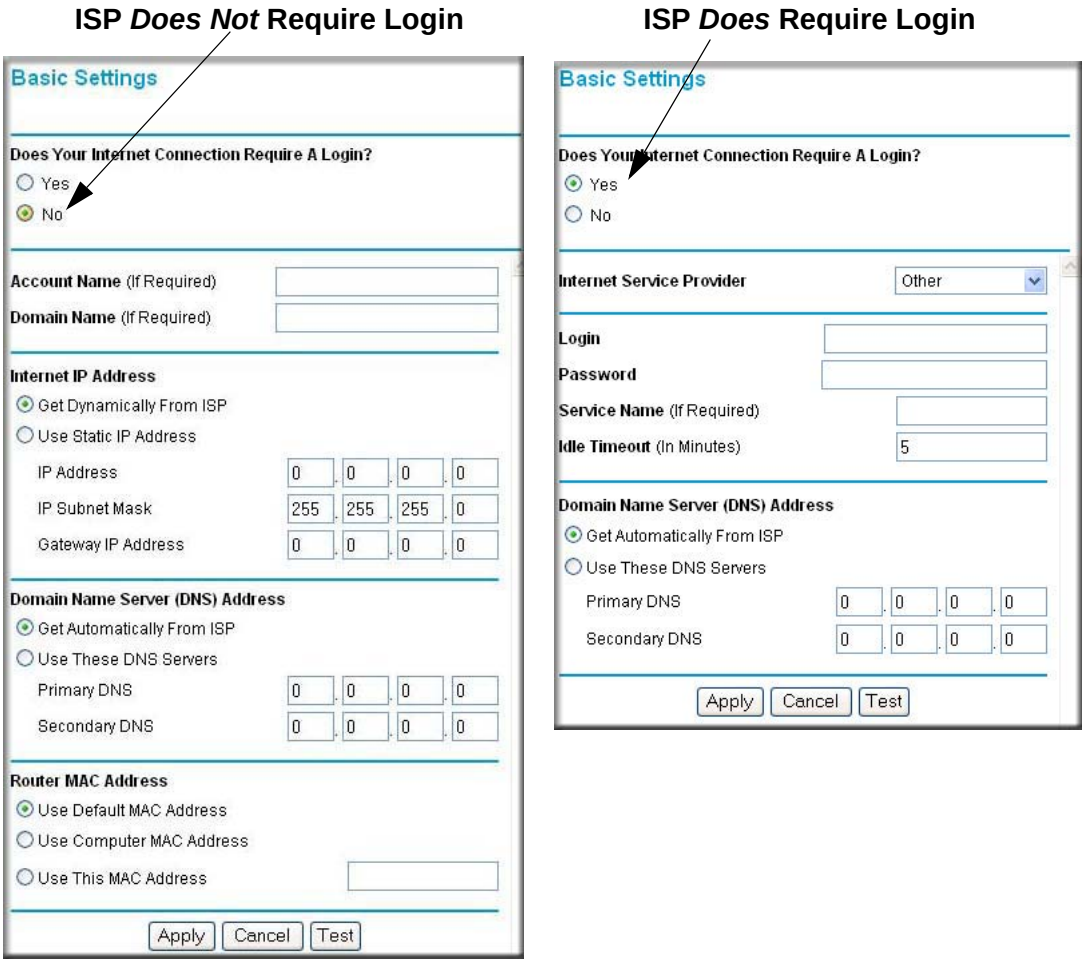


Figure 3-6: Browser-based configuration Basic Settings menus

You can manually configure the router using the Basic Settings menu shown in Figure 3-6 using these steps:

1. Click the Basic Settings link on the Setup menu.

2. If your Internet connection does not require a login, click No at the top of the Basic Settings menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click Yes, and skip to step 3.

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

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

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

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

   d. Gateway's MAC address:
   This section determines the Ethernet MAC address that will be used by the router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your PC when your account is first opened. Then they only accept traffic from the MAC address of that PC. This feature allows your router to masquerade as that PC by "cloning" its MAC address.

      To change the MAC address, select "Use this Computer's MAC address." The router will capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP. Or, select "Use this MAC address" and enter it.

   e. Click Apply to save your settings.

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

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

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

Figure 3-7: Basic Settings ISP list

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

4. If your Internet connection does require a login, fill in the settings according to the instructions below.

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

   a. Select your Internet service provider from the drop-down list. Your choices are:

      - Other — if you have installed PPP software such as WinPoET (from Earthlink) or Enternet (from Pacbell), then select Other. For more information, see "Manual PPPoE Configuration" on page 3-11.
      - PPTP — this protocol is used in Austria and other European countries. For more information, see "Manual PPTP Configuration" on page 3-13.
      - Telstra Bigpond — this protocol is used mainly in Australia. For more information, see "Manual Telstra Bigpond Configuration" on page 3-15.

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

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

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

Manual PPPoE Configuration

If your ISP uses PPPoE, select Other for the Internet Service Provider in the Basic Settings menu to display the following menu:

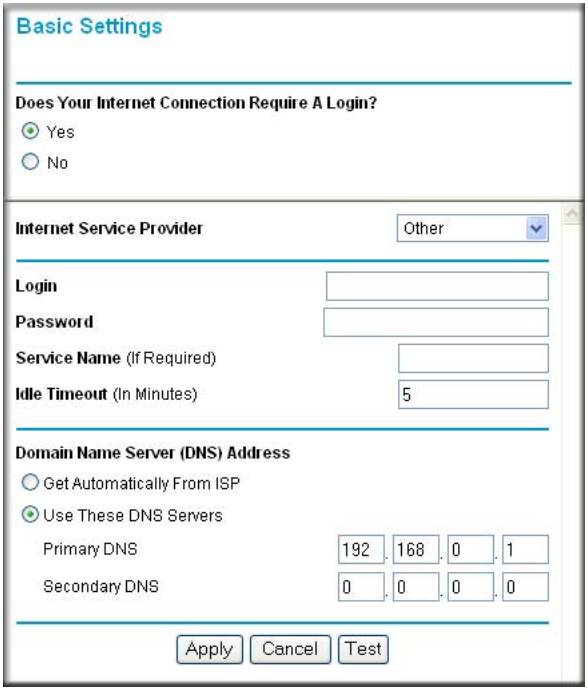


Figure 3-8: Other (PPPoE) menu

To configure your Internet service connection for Other (PPPoE), fill in the following fields:

- Enter the Login and Password as provided by your ISP. These fields are case sensitive.
- To change the login timeout, enter a new value in minutes. This determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a timeout value of zero means never log out.
- If you know that your ISP does not automatically transmit DNS addresses to the router during login, select “Use these DNS servers” and enter the IP address of your ISP’s Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

  Note: If you enter DNS addresses, restart your computers so that these settings take effect.
- Click Apply to save your settings.
- Click Test to verify that your Internet connection works. If the NETGEAR Web site does not appear within one minute, refer to Chapter 8, “Troubleshooting”.

Manual PPTP Configuration

If your ISP uses PPTP, select PPTP for the Internet Service Provider in the Basic Settings menu and you will see the following menu:

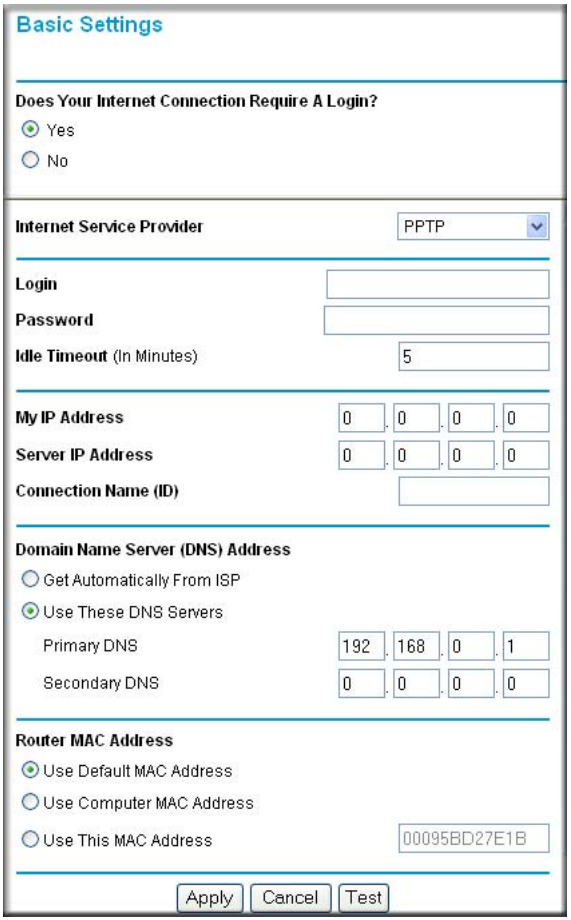


Figure 3-9: PPTP menu

To configure your Internet service connection for PPTP, fill in the following fields:

- Enter your Login and Password. These fields are case sensitive.
- To change the login timeout, enter a new value in minutes. This determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a timeout value of zero means never log out.
- Enter your IP address if your ISP provided a fixed IP address, such as 10.0.1.20. Otherwise, leave the IP address set to 0.0.0.0 and you will be automatically assigned an IP address when you connect.
- Enter a Server IP Address if your ISP provided one, such as 10.0.0.138. Otherwise, leave the IP address set to 0.0.0.0 and the Server IP Address will be automatically supplied when you connect.
- Normally the Connection ID/Name should be left blank. If your ISP provided one, then enter it here.
- If you know that your ISP does not automatically transmit DNS addresses to the router during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

  Note: If you enter DNS addresses, restart your computers so that these settings take effect.

- The Router MAC Address section determines the Ethernet Mac address that will be used by the router on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your router to masquerade as that PC.

  To change the MAC address, select "Use this Computer's MAC address." The router will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP. Or, select "Use this MAC address" and enter it.
- Click Apply to save your settings.
- Click Test to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 8, "Troubleshooting".

Manual Telstra Bigpond Configuration

If your ISP uses Telstra Bigpond, select Telstra Bigpond for the Internet Service Provider in the Basic Settings menu and you will see the following menu:

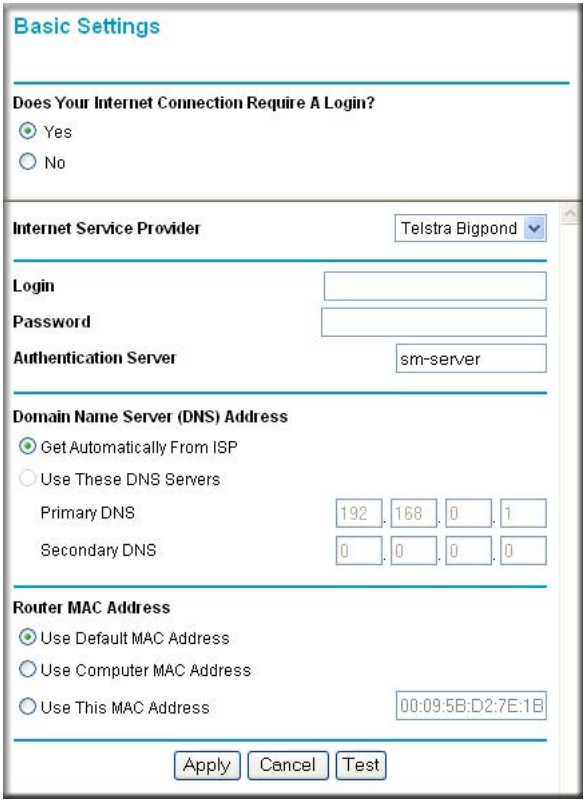


Figure 3-10: Telstra Bigpond Cable menu

To configure your Internet service connection for Telstra Bigpond, fill in the following fields:

- Enter your Login, Password and Authentication Server. These fields are case sensitive.
- If you know that your ISP does not automatically transmit DNS addresses to the router during login, select “Use these DNS servers” and enter the IP address of your ISP’s Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

  Note: If you enter DNS addresses, restart your computers so that these settings take effect.

- The Router Mac Address section determines the Ethernet MAC address that will be used by the router on the Internet port. Some ISPs register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your router to masquerade as that PC.

  To change the MAC address, select "Use this Computer's MAC address." The router will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP. Or, select "Use this MAC address" and enter it.
- Click Apply to save your settings.
- Click Test to test your Internet connection. If the NETGEAR Web site does not appear within one minute, refer to Chapter 8, "Troubleshooting".

Chapter 4
Wireless Configuration

This chapter describes how to configure the wireless features of your WGU624 wireless router. In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your router in order to maximize the network speed. For further information on wireless networking, refer to in Appendix D, "Wireless Networking Basics".

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 router:

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

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

Implementing Appropriate Wireless Security

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

Unlike wired network data, your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WGU624 wireless router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

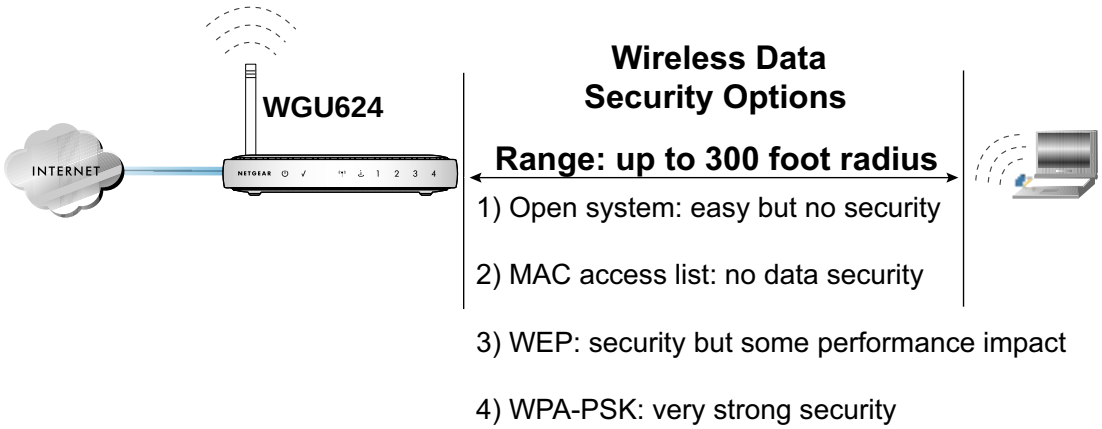


Figure 4-1: WGU624 wireless data security options

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

- **Restrict Access Based on MAC Address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WGU624. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network “discovery” feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.

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

Wireless Mode Options

The following table shows the 802.11a and 802.11b/g settings for each Wireless Mode:

Table 4-1. Wireless Mode Options

Wireless Mode	11a Setting	11g Setting
802.11b/g modes: b only g+b g only Auto Super G 108 Mbps Super G 108 Mbps only	any	 run in 802.11b mode only run in normal g+b mode run in 802.11g mode only run in Auto 108 Mbps run in 108 Mbps only
802.11 a modes: a only Auto Super A 108 Mbps Super A 108 Mbps only	 run in normal a mode only run in Auto 108 Mbps run in 108 Mbps only	any

Default Basic Wireless Settings

When you first receive your WGU624, the default factory settings in effect are shown in the table below. You can restore these defaults with the factory default reset button on the rear panel.

Table 4-2. Default Wireless Settings

FEATURE	DEFAULT SETTINGS
Wireless Access Point	Enabled
Wireless Access List (MAC Filtering)	All wireless stations allowed
SSID broadcast	Enabled
SSID	NETGEAR_11g for 802.11g NETGEAR_11a for 802.11a
11b/g RF Channel	11
11a RF Channel	36
Mode	g and b for 802.11g a only for 802.11a
Authentication Type	WPA-PSK
WPA-PSK passphrase	NETGEAR-ULTRA-G

After you install the WGU624 wireless router, use the procedures below to customize any of the settings to better meet your networking needs.

Basic 802.11a Wireless Settings

To configure the 802.11a wireless settings of your router, click the Wireless a link in the main menu of the browser interface. The Wireless 802.11a Settings menu appears, as shown in “Wireless 802.11a Settings menu” on page 4-5.

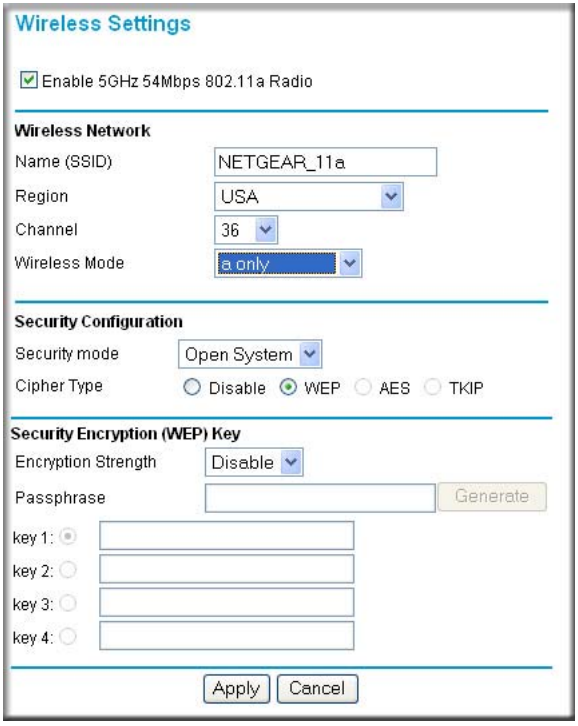


Figure 4-2: Wireless 802.11a Settings menu

The following options are available for the 802.11a configuration:

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 must use this SSID for that network. The WGU624 default SSID is: **NETGEAR_11a**.

Region. This field identifies the region where the WGU624 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 more information on the wireless channel frequencies please refer to “Wireless Channels” on page D-7.

Wireless Mode. This field determines which data communications protocols will be used:

- a only — dedicates the WGU624 to communicating with 802.11a wireless devices exclusively.
- 108 Mbps only — only compatible 802.11a wireless stations that support 108 Mbps can connect.
- Auto 108 Mbps — all 802.11a and NETGEAR 108 Mbps wireless stations can be used.

Security Mode:

- Open System — allows any device to join the network, assuming that the device SSID matches the router SSID. Alternatively, the device can use the "ANY" SSID option to associate with any available router within range, regardless of its SSID.
- Shared Key — only those computers that possess the correct authentication key can join the network.
- 802.1x — defines port-based, network access control used to provide authenticated network access and automated data encryption key management. 802.1x uses a protocol called EAP (Extensible Authentication Protocol).
- WPA-PSK — (Wi-Fi Protected Access Pre-Shared Key) — use WPA standard encryption
- WPA — (Wi-Fi Protected Access) — use WPA standard encryption

Cipher Type:

- Disable
- WEP (Wired Equivalent Privacy) — use WEP 64, 128 or 152 bit data encryption.
- AES — Advanced Encryption Standard, a symmetric 128-bit block data encryption technique. It is an iterated block cipher with a variable block length and a variable key length.
- TKIP — the Temporal Key Integrity Protocol mechanism shares a starting key between devices. Each device then changes its encryption key for every packet.

Basic 802.11g Wireless Settings

To configure the 802.11 g wireless settings of your router, click the Wireless g link in the main menu of the browser interface. The Wireless 802.11g Settings menu appears, as shown below.

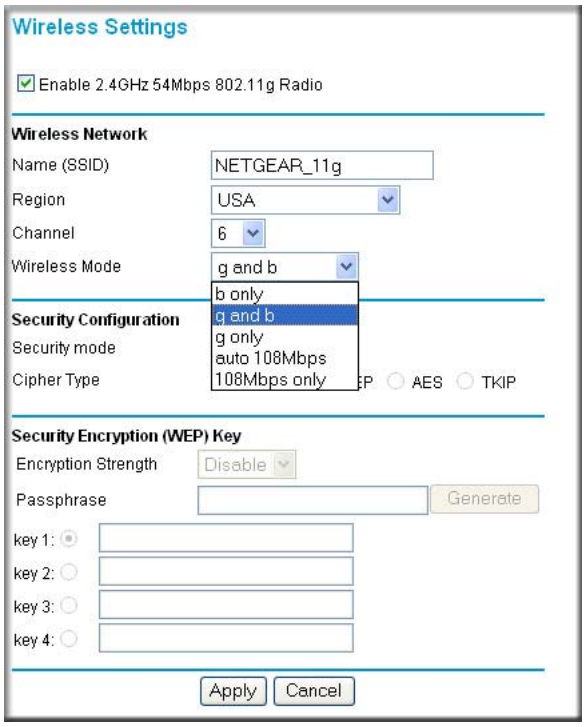


Figure 4-3: Wireless 802.11g Settings menu

The following options are available for the 802.11g configuration:

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 must use this SSID for that network. The WGU624 default SSID is: **NETGEAR_11g**.

Region. This field identifies the region where the WGU624 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 more information on the wireless channel frequencies please refer to “Wireless Channels” on page D-7.

Wireless Mode. This field determines which data communications protocols will be used:

- g & b — both 802.11g and 802.11b wireless stations can be used.
- g only — only 802.11g wireless stations can be used.
- b only — all 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.
- 108 Mbps only — only compatible 802.11g wireless stations that support 108 Mbps can connect.
- Auto 108 Mbps — all 802.11g, 802.11b and NETGEAR 108 Mbps wireless stations can be used.

Note: If you select 108 Mbps mode, the router will only use channel 6.

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

Security Mode:

- Open System — allows any device to join the network, assuming that the device SSID matches the router SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available router within range, regardless of its SSID.
- Shared Key — only those computers that possess the correct authentication key can join the network.
- 802.1x — defines port-based, network access control used to provide authenticated network access and automated data encryption key management. 802.1x uses a protocol called EAP (Extensible Authentication Protocol).
- WPA-PSK — (Wi-Fi Protected Access Pre-Shared Key) — use WPA standard encryption.
- WPA — (Wi-Fi Protected Access) — use WPA-PSK standard encryption.

Cipher Type:

- Disable — no data encryption
- WEP (Wired Equivalent Privacy) — use WEP 64, 128 or 152 bit data encryption.
- AES — Advanced Encryption Standard, a symmetric 128-bit block data encryption technique. It is an iterated block cipher with a variable block length and a variable key length.
- TKIP — the Temporal Key Integrity Protocol mechanism shares a starting key between devices. Each device then changes its encryption key for every packet.

Wireless Security Settings

The following table shows the 11a and 11g security mode and cipher type options:

Table 4-3. Wireless Security Settings

Security Mode	Cipher Type
Open System	WEP — 64, 128, or 152 bit encryption
Shared Key	WEP — 64, 128, or 152 bit encryption
802.1x	none
WPA-PSK	AES or TKIP
WPA	AES or TKIP

Instructions on how to configure the security settings are provided in the following sections.

WEP Authentication and Encryption

Restricting wireless access to your network prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the WEP data encryption settings described below will prevent a determined intruder from eavesdropping on your wireless data communications. Also, if you are using the Internet for such activities as purchases or banking, those Internet sites use another level of highly secure encryption called SSL. You can tell if a Web site is using SSL because the Web address begins with HTTPS rather than HTTP.

Security Mode Selection

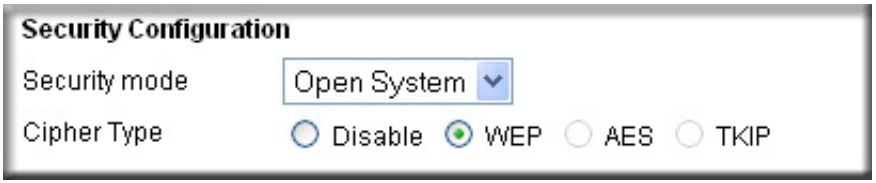


Figure 4-4: Encryption Strength

The WGU624 lets you select the following wireless security modes with the WEP Cypher Type:

- **Open System**. With Open Network Authentication and 64-, 128-, or 152- bit WEP data encryption, the WGU624 performs data encryption, but does not perform any authentication.
- **Shared Key.** Encrypts the SSID and data. Choose the Encryption Strength (64-, 128-, or 152-bit data encryption). Manually enter the key values or enter a word or group of printable characters in the Passphrase box. Manually entered keys are case sensitive but Passphrase characters are not case sensitive.

Note: Not all wireless adapter configuration utilities support Passphrase key generation.

	**Note:** The security mode is separate from the data encryption cipher type. You can choose the Shared Key security mode, but still leave the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

Be sure to set your wireless adapter according to the authentication scheme you choose for the WGU624 wireless router. Please refer to “Authentication and WEP” on page D-3 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

Cipher Type Choices

Choose the encryption strength from the drop-down list. Please refer to “Overview of WEP Parameters” on page D-5 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

- **Disable.** No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.
- **64-bit, 128-bit, or 152-bit WEP.** When selected, WEP encryption will be applied. If encryption strength is set to 128 bit or 152 bit, then only the selected WEP key box will automatically be populated with key values.

If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and access points in your network.

There are two methods for creating WEP encryption keys:

- **Passphrase**. Enter a word or group of printable characters in the Passphrase box and click the Generate button. These characters *are* case sensitive.
- **Manual**. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F). For 152-bit WEP, enter 32 hexadecimal digits (any combination of 0-9, a-f, or A-F). These values *are not* case sensitive.

WPA Encryption

You can select WPA-PSK or WPA for the Security Mode. The default is WPA-PSK. WPA-Pre-shared Key performs authentication, uses 128-bit data encryption and dynamically changes the encryption keys, making it nearly impossible to circumvent.

You must use the same wireless security settings on the client adapters to properly implement WPA security.

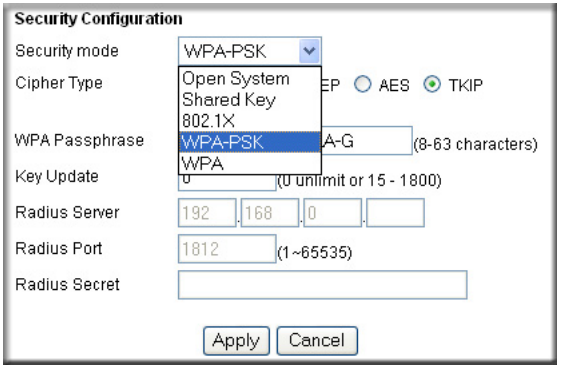


Figure 4-5: Security Modes

Cipher Type Choices

- **AES.** Advanced Encryption Standard, a symmetric 128-bit block data encryption technique. It is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128, 192 or 256 bits.The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.
- **TKIP**. The Temporal Key Integrity Protocol mechanism shares a starting key between devices. Each device then changes their encryption key for every packet. It is extremely difficult for hackers to read messages — even if they have intercepted the data.

Passphrase

The Passphrase must be identical on all PCs and access points in your network. Enter a word or group of printable characters in the Passphrase box. These characters are case sensitive.

Key Update

The default Key Update is 0 for unlimited updates. You can change this to a value between 15 and 1800.

Radius Server Settings

- Enter the Radius Server IP address.
- The Radius Port number is 1812 by default.
- Enter a Radius Secret, which can be up to 32 alphanumeric characters

Note: Not all wireless adapter configuration utilities support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.

Recording Your SSID and Security Settings

Before customizing your wireless settings, print this form and record the following information.

802.11a Wireless Network Name (SSID):_____

802.11g Wireless Network Name (SSID):_____

The Service Set Identification (SSID), called the wireless network name in Windows XP, identifies the wireless network. You may use up to 32 alphanumeric characters. The SSID in the wireless router is the SSID you configure in the wireless adapter card. For the access point and wireless nodes to communicate with each other, all must be configured with the same 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 set to Shared Key as well.

— **WEP Encryption Strength**. Choose the key size. Circle one: **64**, **128, or 152** bit.

— **Data Encryption (WEP) Keys**. The WGU624 provides two methods for creating WEP encryption keys:

- **Passphrase**. _____ Enter a word or group of printable characters. These characters *are* case sensitive. When you enter the Passphrase and click the Generate button on the WGU624, the keys will be generated.
- **Manual**. For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0-9 or a-f). These values *are not* case sensitive. For 128-bit WEP, enter 26 hex digits. For 152-bit WEP, enter 32 hex digits. Record the key values in the spaces below.

Key 1: _____ **Key 3:**_____

Key 2: _____ **Key 4:**_____

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

— **Passphrase**. _____

Store this information in a safe place. Use the procedures described in the following sections to configure the WGU624.

Setting Up and Testing 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 WGU624 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 a or g Settings link in the main menu of the WGU624.

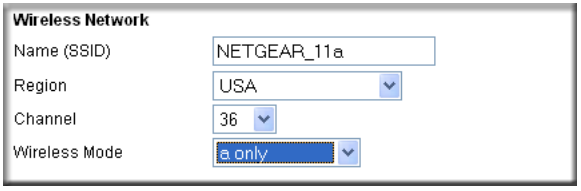


Figure 4-6: Wireless Settings menu

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_11a for 802.11a and NETGEAR_11g for 802.11g.

   Note: The SSID of any wireless access adapters must match the SSID you configure in the Double 108 Mbps Wireless Firewall Router WGU624. If they do not match, you will not get a wireless connection to the WGU624.

4. Set the Region. Select the region in which the wireless interface will operate.
5. Set the 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 wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your router. For more information on the wireless channel frequencies please refer to “Wireless Channels” on page D-7.

6. For initial configuration and test, leave the Cipher Type set to “Disabled”.
7. Click Apply to save your changes.

	**Note:** If you are configuring the router from a wireless PC 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 PC to match the router's new settings.

8. Configure and test your PCs for wireless connectivity.

   Program the wireless adapter of your PCs 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 router.

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

Restricting Wireless Access by MAC Address

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

1. Log in to the WGU624 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 router from a wireless PC 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 on Apply. You must then access the wireless router from a wired PC or from a wireless PC which is on the access control list to make any further changes.

2. Click the Advanced Wireless a or Advanced Wireless g Settings link in the main menu of the WGU624 wireless router.

3. Click the Setup Access List button to display the Wireless Card Access menu shown below.

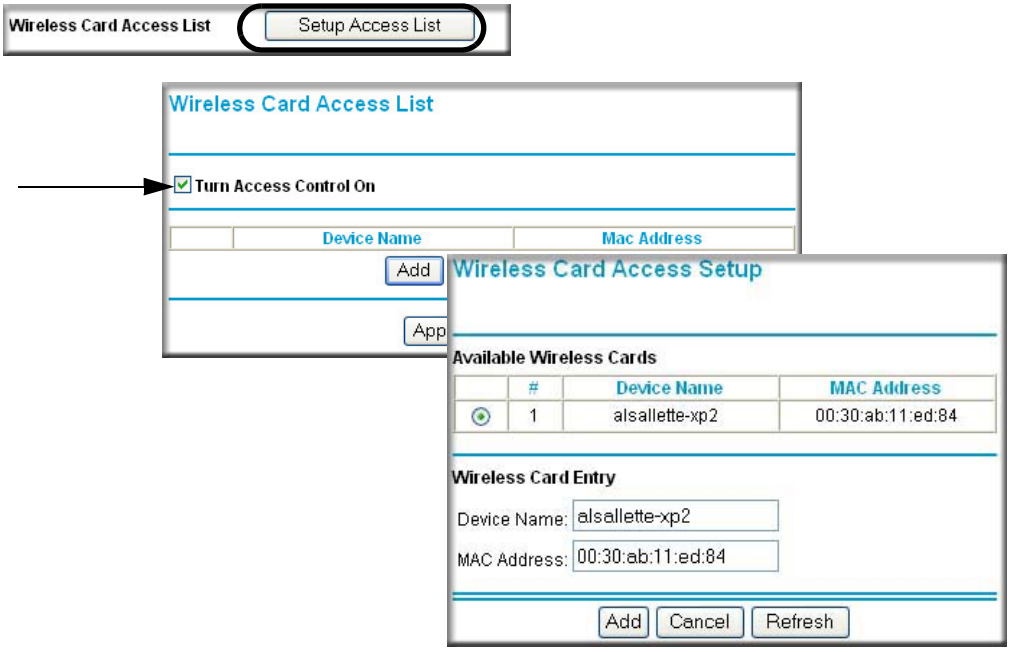


Figure 4-7: Wireless Card Access List Setup

4. Click Add to add a wireless device to the wireless access control list. The Available Wireless Cards list displays.
5. Click the Turn Access Control On check box.
6. Then, either select from the list of available wireless cards the WGU624 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 router's Attached Devices menu into the MAC Address box of this menu. To do this, configure each wireless PC to obtain a wireless link to the router. The PC 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. Be sure to click Apply to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the WGU624.

Configuring WEP

To configure WEP data encryption, follow these steps:

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

1. Log in to the WGU624 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 a or g link in the main menu of the WGU624.
3. From the Security Encryption menu drop-down list, select the WEP encryption strength you will use.

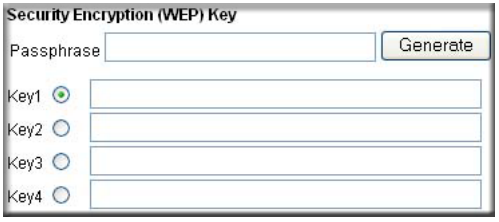


Figure 4-8. Wireless Security Encryption menu

4. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.
   - Automatic — enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
   - Manual — enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F)
     Select which of the four keys will be active.

   Please refer to "Overview of WEP Parameters" on page D-5 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.
5. Click Apply to save your settings.

Configuring WPA-PSK Encryption Security

Wi-Fi Protected Access (WPA) is wireless security with far greater protection than WEP. WPS-PSK (pre-shared key) uses encryption of a shared key as the starting point. WPA has a significant advantages over WEP — an encryption key differing in every packet. It is extremely difficult for hackers to read messages even if they have intercepted the data.

To enable WPA-PSK Encryption Security:

1. Click the Wireless Settings a or g link in the main menu of the WGU624 wireless router.
2. Select WPA-PSK.

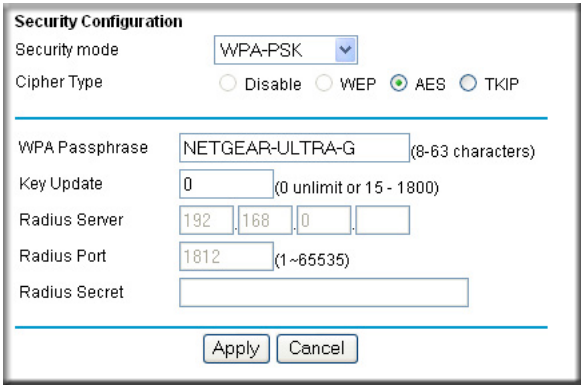


Figure 4-9: WPA-PSK Security Configuration

3. For the Cipher Type, select AES or TKIP.
4. Enter a Passphrase. The Passphrase can be between 8 and 63 characters. The default Passphrase is **NETGEAR-ULTRA-G**.
5. The default for the Key Update time is 0, which is unlimited. If you want to limit the key Update period, select a value between 15 and 1800 seconds.
6. Click Apply.

For more information on WPA security, see “WPA Wireless Security” on page D-8.

Configuring Advanced Wireless Settings

The advanced wireless settings are configured separately for the 802.11a and 802.11g protocols.

Default Advanced Wireless Settings

The default advanced wireless settings are shown in the table below.

Note: These settings should work for most networks and should not be changed unless you have a specific reason to do so.

Table 4-4. Default Advanced Wireless Settings

FEATURE	802.11a	802.11g
SSID Broadcast	Enabled	Enabled
Super A / Super G mode	Enabled	Enabled
eXtended Range	Enabled	Enabled
Adaptive Radio	not applicable	Disabled
Transmit Power	Max	Max
Fragmentation Threshold	2346	2346
CRS/RTS Threshold	2346	2346
Preamble Mode	Automatic	Automatic
DTIM	1	1

Configuring Advanced 802.11a Wireless Settings

From the main menu, click Advanced a Wireless Settings to view the configuration menu shown below.

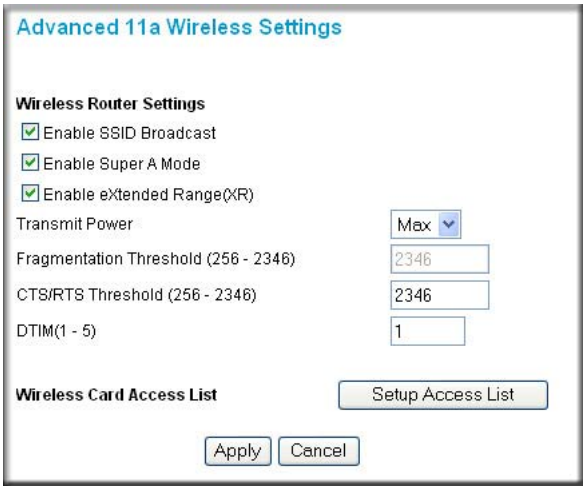


Figure 4-10: Advanced 802.11a Wireless Settings

- Enable SSID Broadcast — allow Broadcast of Network Name (SSID). If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network 'discovery' feature of some products such as Windows XP.
- Enable Super A Mode — if enabled, the Wireless Router will enable data compression, packet bursting and large frame support.
- Enable eXtended Range — eXtended Range (XR) technology provides significantly longer range than basic 802.11 by maintaining connectivity when signals are made fainter when passing through dense walls, floors, or other barriers. XR products require no additional configuration and are fully interoperable with standard 802.11 technologies.

Note: The XR feature is NOT available when the wireless mode is "108Mbps only".

- Transmit Power — Max, 75%, 50%, 25%, or Min. The default is Max.
- Fragmentation Threshold — value can be from 256 to 2346. The default is 2346.
- CRS/RTS Threshold — value can be from 256 to 2346. The default is 2346.

- DTIM — from 1 to 5. The default is 1. DTIM stands for Delivery Traffic Indication Message. This setting determines how often the Access Point's Beacon (Traffic Indication Message) contains a DTIM. The DTIM tells client devices in power-save mode that a packet is waiting for them. The default setting causes client devices using power-save mode to wake up. To conserve battery power in client devices using power-save mode, increase the Data Beacon Rate (DTIM) setting. However, setting the DTIM too high may cause a wireless client to lose its network connection.
- Wireless Card Access List — when the Trusted PCs Only radio button is selected, the WGU624 checks the MAC address of the wireless station and only allows connections to PCs identified on the trusted PCs list.

Configuring Advanced 802.11b/g Wireless Settings

From the main menu, click Advanced g Wireless Settings to view the configuration menu shown below.

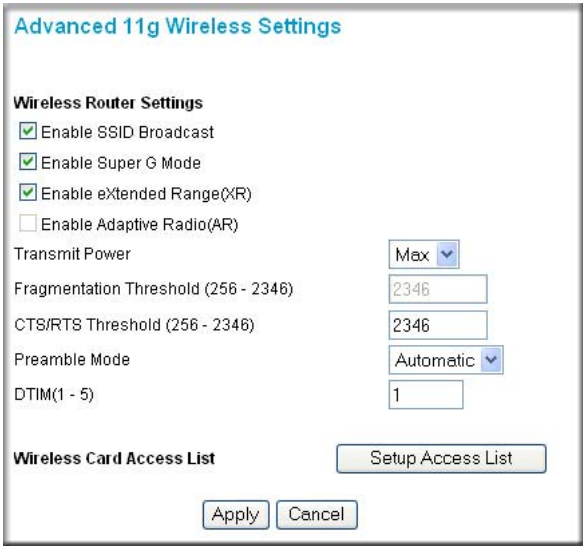


Figure 4-11: Advanced 802.11g Wireless Settings

- Enable SSID Broadcast — allow broadcast of the Network Name (SSID). If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network ‘discovery’ feature of some products such as Windows XP.

- Enable Super G Mode — if enabled, the wireless router will enable data compression, packet bursting and large frame support.
- Enable eXtended Range — eXtended Range (XR) technology provides significantly longer range than basic 802.11 by maintaining connectivity when signals are made fainter when passing through dense walls, floors, or other barriers. XR products require no additional configuration and are fully interoperable with standard 802.11 technologies.

Note: The XR feature is NOT available when the wireless mode is “108Mbps only” and “b only”.

- Enable Adaptive Radio — the Adaptive Radio (AR) feature is an option that is available when the wireless settings are switched to the Auto 108 mode. When enabled, the Auto 108 mode slows the data rate down automatically to the standard 802.11g (11g or 11b) mode and operate at 54 Mbps or below when it senses any other neighboring wireless networks that are using adjacent wireless channels. It steps up to a maximum data rate of 108 Mbps when it senses that no other neighboring wireless networks are using adjacent channels. NETGEAR 108 Mbps Wireless Products provide minimum interference to neighboring networks, so the default setting for the Adaptive Radio feature is set to “Disable”.
- Transmit Power —Max, 75%, 50%, 25%, or Min. The default is Max.
- Fragmentation Threshold — value can be from 256 to 2346. The default is 2346.
- CRS/RTS Threshold — value can be from 256 to 2346. The default is 2346.
- Preamble Mode — Automatic or Long. The default is Automatic. Most access points and client adapters have a setting called Preamble Type — Short or Long. The default “Automatic” will automatically pick Short or Long preamble type depending on the client capability.
- DTIM — from 1 to 5. The default is 1. DTIM stands for Delivery Traffic Indication Message. This setting determines how often the Access Point's Beacon (Traffic Indication Message) contains a DTIM. The DTIM tells client devices in power-save mode that a packet is waiting for them. The default setting causes client devices using power-save mode to wake up. To conserve battery power in client devices using power-save mode, increase the Data Beacon Rate (DTIM) setting. However, setting the DTIM too high may cause a wireless client to lose its network connection.
- Wireless Card Access List — when the Trusted PCs Only radio button is selected, the WGU624 checks the MAC address of the wireless station and only allows connections to PCs identified on the trusted PCs list.

Chapter 5
Content Filtering

This chapter describes how to use the content filtering features of the Double 108 Mbps Wireless Firewall Router WGU624 to protect your network. These features can be found by under the Content Filtering heading in the main menu of the browser interface.

The Double 108 Mbps Wireless Firewall Router WGU624 provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Web addresses and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

Blocking Access to Internet Sites

The WGU624 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.

To block access to Internet Sites, select Block Sites under the Content Filtering heading in the main menu of the Web browser interface.

Keyword application examples:

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

The Block Sites menu is shown below:

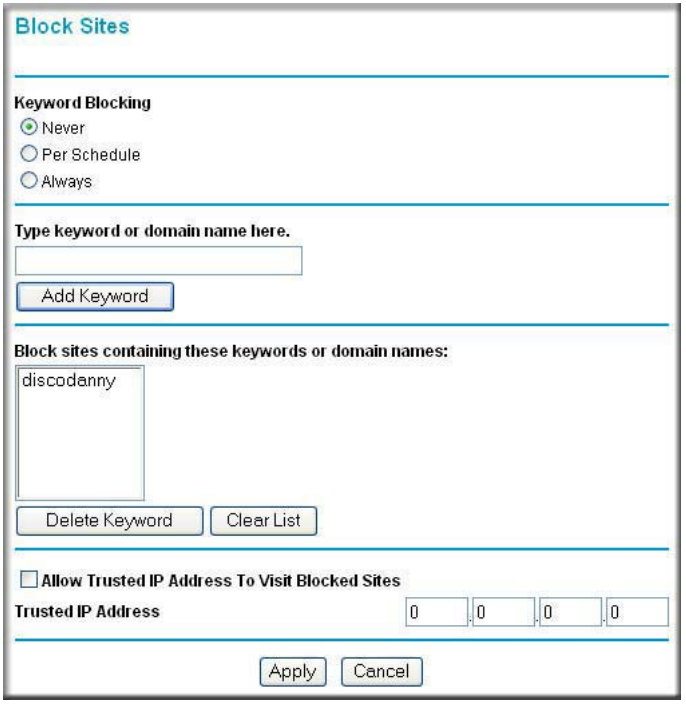


Figure 5-1: Block Sites menu

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.

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

Blocking Access to Internet Services

The WGU624 wireless router allows you to block the use of certain Internet services by PCs on your network. This is called services blocking or port filtering. The Block Services menu is shown below:

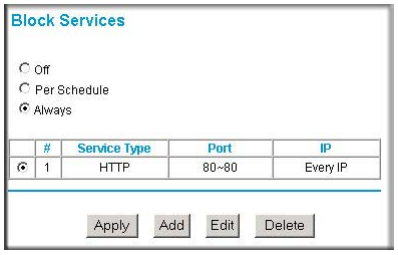


Figure 5-2: Block Services menu

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 is shown below:

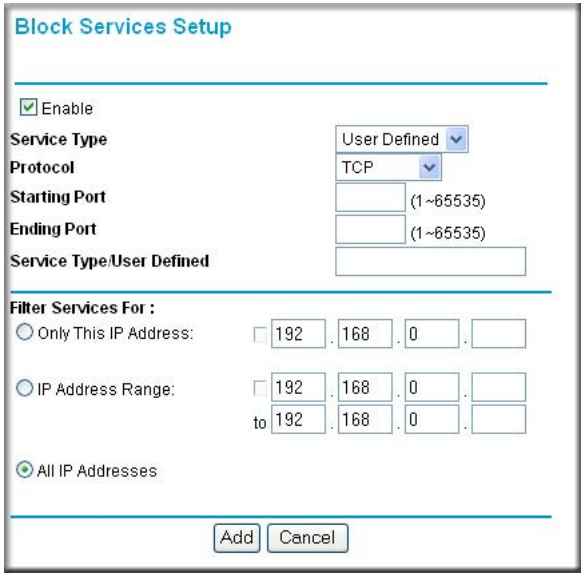


Figure 5-3: Block Services Setup menu

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

Configuring a User Defined Service

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

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

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

Configuring Service Blocking by IP Address Range

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

Scheduling When Blocking Will Be Enforced

The WGU624 wireless router allows you to specify when blocking will be enforced. The Schedule menu is shown below:

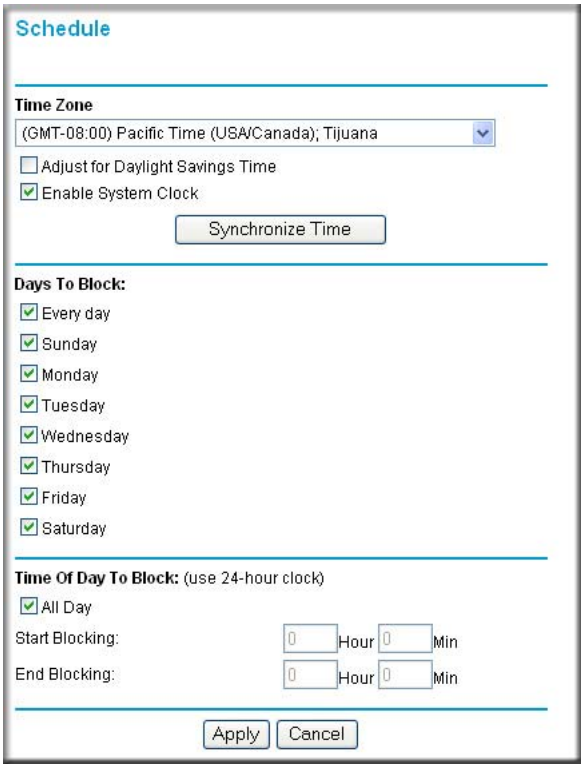


Figure 5-4: Schedule menu

Use the check boxes on this menu to create a schedule for blocking content. Then click Apply.

Time Zone. Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.

Adjust for Daylight Savings Time. If your region uses Daylight Savings Time, you must manually select Adjust for Daylight Savings Time on the first day of Daylight Savings Time, and clear this check box at the end. Enabling Daylight Savings Time will cause one hour to be added to the standard time.

Enable System Clock. Uses the system clock in the router.

Synchronize Time. Syncs up the router time with a NETGEAR time server, so that the Logs, e-mail timestamps and other information will have the current time.

Days to Block. Select days to block by checking the appropriate boxes. Select Everyday to check the boxes for all days. Click Apply.

Time of Day to Block. Select a start and end time in 23:59 format. Select All day for 24 hour blocking. Click Apply.

Viewing Logs of Web Access or Attempted Web Access

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

Figure 5-5: Logs menu

Log entries are described in Table 5-1

Table 5-1. Log entry descriptions

Field	Description
Number	The index number of the content filter log entries. Up to 128 entries are available numbered from 0 to 127. The log keeps a record of the latest 128 entries.
Action	This field displays whether the access was blocked or allowed.
Web site	The name or IP address of the Web site 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 5-2

Table 5-2. Log action buttons

Button	Description
Refresh	Refresh the log screen.
Clear Log	Clear the log entries.
Send Log	E-mail the log immediately.

Configuring E-Mail Alert and Web Access Log Notifications

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

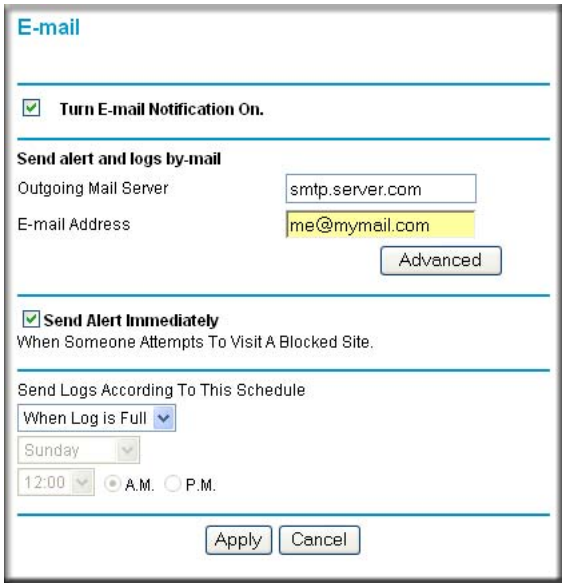


Figure 5-6: E-mail menu

Turn E-mail notification on: Select this check box if you wish to receive e-mail logs and alerts from the router.

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.

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.

Sending Alerts and Logs

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

- **Send alert immediately**
  Select this check 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, it is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents. If you do not want logs sent, select None. 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.

Chapter 6
Maintenance

This chapter describes how to use the maintenance features of your Double 108 Mbps Wireless Firewall Router WGU624. These features can be found by clicking on the Maintenance heading in the main menu of the browser interface.

Viewing Wireless Router Status Information

The Router Status menu provides a limited amount of status and usage information. From the main menu of the browser interface, click Router Status to view the status screen, shown below.

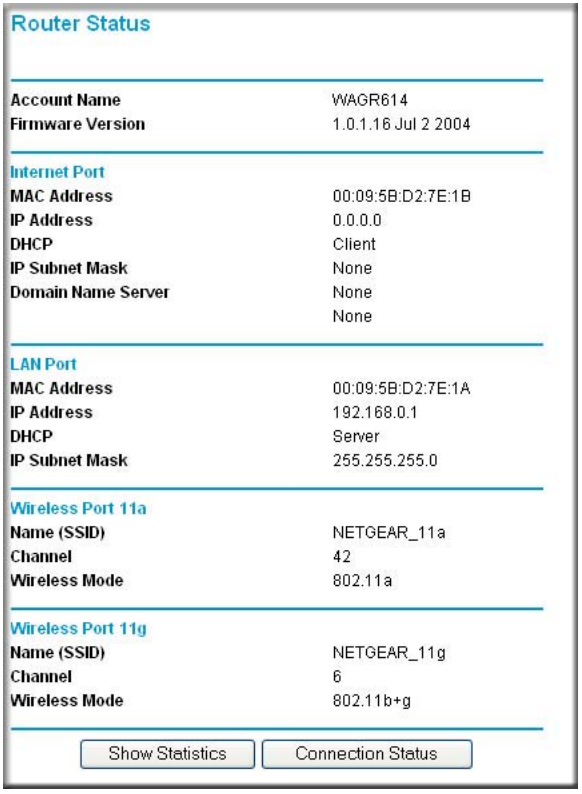


Figure 6-1: Router Status screen

The Router Status screen displays the following parameters:

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

Field	Description
Account Name	The Host Name assigned to the router.
Firmware Version	The router firmware version.
Internet Port	These parameters apply to the Internet (WAN) port of the router.
MAC Address	The Media Access Control address being used by the Internet (WAN) port of the router.
IP Address	The IP address used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet.
IP Subnet Mask	The IP Subnet Mask used by the Internet (WAN) port of the router.
DHCP	If set to None, the router is configured to use a fixed IP address on the WAN. If set to Client, the router is configured to obtain an IP address dynamically from the ISP.
LAN Port	These parameters apply to the Local (LAN) port of the router.
MAC Address	The Media Access Control address used by the LAN port of the router.
IP Address	The IP address used by the Local (LAN) port of the router. The default is 192.168.1.1.
DHCP	Identifies if the router's built-in DHCP server is active for the LAN attached devices.
IP Subnet Mask	The IP Subnet Mask used by the Local (LAN) port of the router. The default is 255.255.255.0
Wireless Port A	These parameters apply to the Wireless a port of the router.
Name (SSID)	The wireless network name (SSID) being used by the wireless port of the router. The default is NETGEAR_11a.
Channel	Identifies if the channel the wireless port is using. See "Wireless Channels" on page D-7 for the frequencies used on each channel.
Wireless Mode	802.11a, 108 Mbps, or Auto
Wireless Port G	These parameters apply to the Wireless g port of the router.
Name (SSID)	The wireless network name (SSID) used by the wireless port of the router. The default is NETGEAR_11g.
Channel	Identifies if the channel the wireless port is using. See "Wireless Channels" on page D-7 for the frequencies used on each channel.
Wireless Mode	802.11b+g, b only, g only, 108 Mbps, or Auto

From the Router Status screen, click the “Connection Status” button to display the connection status, as shown below.

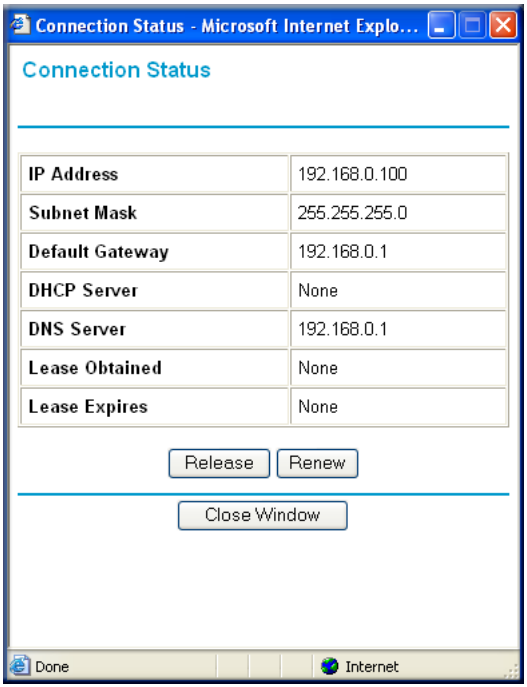


Figure 6-2: Connection Status screen

This screen shows the following statistics:.

Table 6-1. Connection Status Fields

Field	Description
IP Address	The WAN (Internet) IP Address assigned to the router.
Subnet Mask	The WAN (Internet) Subnet Mask assigned to the router.
Default Gateway	The WAN (Internet) default gateway the router communicates with.
DHCP Server	The DHCP server on the network.
DNS Server	The DNS server on the network.
Lease Obtained	The length of time the router has been connected to your Internet service provider’s network.
Lease Expires	The time the lease expires.

Click the Renew button to renew the DHCP lease.

From the Router Status screen, click the “Show Statistics” button to display router usage statistics, as shown below.

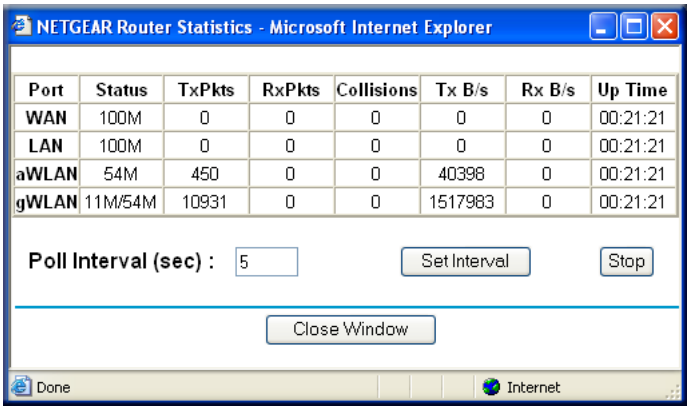


Figure 6-3: Router Statistics screen

This screen shows the following statistics:

Table 6-1. Router Statistics Fields

Field	Description
Port	The statistics for the WAN (Internet) and LAN (local) ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the WAN and LAN ports.
Rx B/s	The current reception (inbound) bandwidth used on the WAN and LAN ports.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click Stop to freeze the display.

Show Statistics action buttons are described in Table 6-2.

Table 6-2. Show Statistics action buttons

Field	Description
Set Interval	Enter a time and click the button to set the polling frequency.
Stop	Click the Stop button to freeze the polling information.

Viewing a List of Attached Devices

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

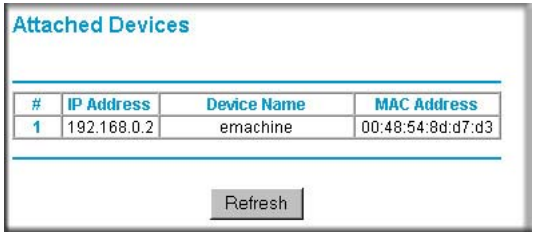


Figure 6-4: Attached Devices menu

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

Upgrading the Router Software

The routing software of the WGU624 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 WGU624 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://kbserver.netgear.com/products/WGU624.asp*.

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

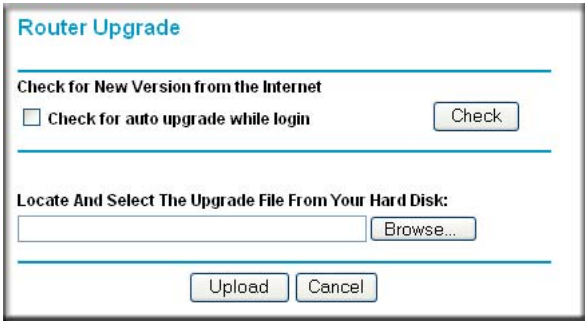


Figure 6-5: Router Upgrade menu

Note: When uploading software to the WGU624 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:

1. Click Check. If the WGU624 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 the Browse button and browse to the location of the upgrade file.
2. Click Upload.

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

Configuration File Management

The configuration settings of the WGU624 wireless router are stored within the router in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

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

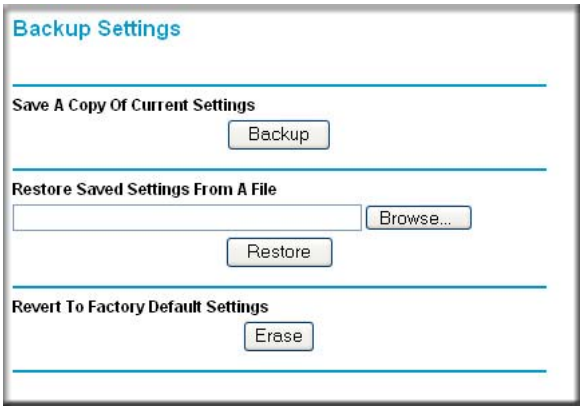


Figure 6-6: Backup Settings menu

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

Restoring and Backing Up the Configuration

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

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

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

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

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 bring up the menu shown below.

Figure 6-7: Set Password menu

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 Double 108 Mbps Wireless Firewall Router WGU624. These features can be found under the Advanced heading in the main menu of the browser interface.

Comparison of Port Triggering and Port Forwarding

Port Triggering 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.

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

- Port Forwarding is designed for FTP, Web Server or other server based services. Once port forwarding is set up, requests from the Internet are forwarded to the proper server.
- Port triggering only allows requests from the Internet after a designated port is 'triggered'. Port triggering applies to chat and Internet games.
  - Port Triggering opens an incoming port temporarily and does not require the server on the Internet to track your IP address if it is changed by DHCP, for example.
  - Port Triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and “triggers” the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

Configuring Port Forwarding

For the services, applications, or games, that already exist in the pull-down list, you only need to specify the computer's IP address. Otherwise, the port number and computer's IP address for each service, game or application should be specified by clicking the Add Custom Service button.

Port Assignment

You can make up to 20 different port assignments for Internet services, applications or games. In the Service Name lists, you can select either a service, application or game. If you do not see an item that you want to use in any of the lists, check with the software or game developer for the correct port numbers to use.

For Internet Services

Before starting, you need to determine which type of services you will provide and the IP address of the computer that will provide those services. The most common services you would provide are a Web (HTTP) server or FTP server.

To set up a computer or server to be accessible to the Internet for an Internet service:

1. From the main menu, under the Advanced heading, select Port Forwarding/Port Triggering.
2. Select Port Forwarding to display the menu shown below:

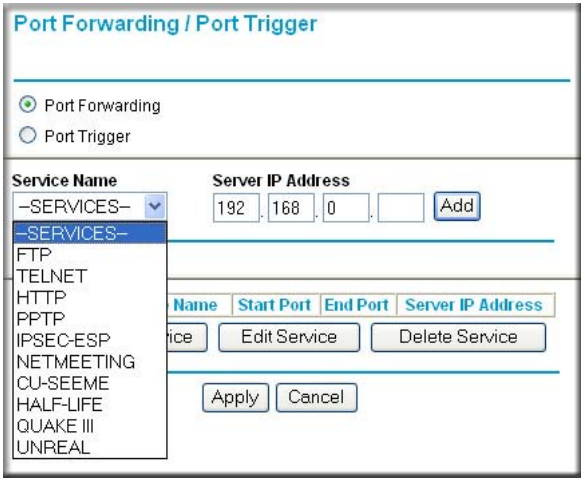


Figure 7-1: Port Forwarding Menu

3. Select the Internet service you want to use from the Service Name list. If the service does not appear in the list, refer to the section "Adding a Port Forwarding Custom Service" on page 7-3.
4. Type the IP address of the computer in the Server IP Address box.
5. Click the Add button.

Note: You may have a single computer or server available for more than one type of service. To do that, select another service, and type the same IP address for that computer or server.

For Internet Games or Applications

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.

Note: If you are unfamiliar with networking and routing, refer to Appendix B, "Network, Routing, Firewall, and Basics", to become more familiar with the terms and procedures used in this manual.

Use the Port Forwarding menu to configure the router to forward incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded. The DMZ server must be connected to LAN port 4 on the WGU624. The DMZ port feature can be enabled in the WAN Setup menu. See "Configuring WAN Setup Options" on page 7-6 for more information.

Before starting, you need to determine which type of service, application or game you will provide and the IP address of the computer that will provide 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.
2. Enter the IP address of the local server in the corresponding Server IP Address box.
3. Click the Add button.

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 which port numbers are used by the service. For this information, you may need to contact the manufacturer of the program that you want to use. When you have the port number information, follow these steps:

1. Click the Add Custom Service button.
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.

Adding Additional Computers

To set up an additional computer to play, for example Hexen II or KALI:

1. Click the Add Custom Service button.
2. Type the service name in the Service Name box.
3. Type the beginning port number in the Starting Port box.

   For these games, use the supplied number in the default listing and add +1 for each additional computer. For example, if you have already configured one computer to play Hexen II using port 26900, the second computer's port number would be 26901, the third computer's port number would be 26902.
4. Type the same port number in the Ending Port box.
5. Type the IP address of the computer in the Server IP Address box.
6. Click the Add button.

Local Web and FTP Server Example

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

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

Some considerations for this application are:

- If your account’s IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires.

- If the IP address of the local PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, you can manually configure the PC to use a fixed address.
- Local PCs must access the local server using the PCs' local LAN address (192.168.1.33 in this example). Attempts by local PCs to access the server using the external IP address (172.16.1.23 in this example) will fail.

Some online games and videoconferencing applications are incompatible with NAT. The WGU624 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 PC can run the application properly if that PC's IP address is entered as the default in the Port Forwarding Menu. If one local PC acts as a game or videoconferencing host, enter its IP address as the default.

Configuring Port Triggering

To define a game or application for Port Triggering, 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. From the main menu of the browser interface, under the Advanced section, select Port Forwarding/Port Triggering.
2. Select Port Triggering to display the Port Triggering screen, as shown below.

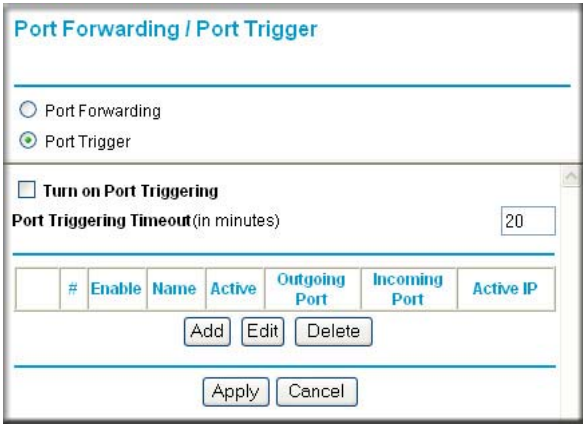


Figure 7-2: Port Triggering menu

3. Click the Add button.
4. Type a name for the service.
5. Enter unused port numbers for the Outgoing Start Port and End Port. To trigger only one port, enter it again in the Outgoing End Port box. To specify a range of ports, enter the last port to be triggered in the End Port box.
6. Enter unused port numbers for the Incoming Start Port and End Port. To trigger only one port, enter it again in the Incoming End Port box. To specify a range of ports, enter the last port to be forwarded in the End Port box.
7. Enter the IP address of the local server or computer in the corresponding Server IP Address box.
8. Click Add.
9. Select the Turn on Port Triggering check box.
10. Specify the Port Triggering Timeout value.
11. Click Apply at the bottom of the menu to save your new configuration.

Configuring WAN Setup Options

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

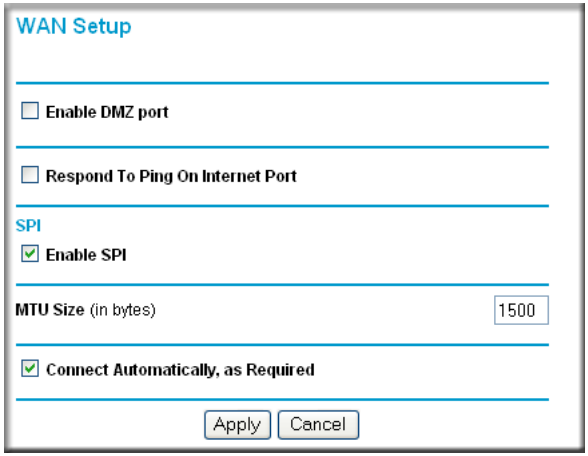


Figure 7-3: WAN Setup menu.

Enable DMZ Port: LAN port 4 on the WGU624 is reserved to be used as the DMZ port. You can also use this port as a regular LAN port when this feature is not enabled. The DMZ port 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 PC can run the application properly if that PC is connected directly to LAN port 4 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. However, the WGU624 provides a hardware DMZ port, which is much more secure than a software solution. When enabled, the DMZ port is in a separate LAN sector from the other LAN ports, including the Wireless LAN.

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.

To forward traffic to the DMZ server:

1. From the Main Menu of the browser interface, under Advanced, click Port Forwarding/Port Triggering.
2. Select Port Forwarding to display the Port Forwarding menu.
3. Select the Internet service you want to forward from the Service Name list. If the service does not appear in the list, refer to the section “Adding a Port Forwarding Custom Service” on page 7-3.
4. Enter the IP address of the DMZ server in the corresponding Server IP Address box.
5. Click Apply at the bottom of the menu.

Respond to Ping on Internet Port: If you want the router to respond to a 'ping' from the Internet, select the Respond to Ping on Internet Port check box. This should 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.

Disable SPI: Normally, this option should be Enabled, so that your local network will be protected by the Stateful Packet Inspection (SPI) firewall included in the WGU624. However, certain communications functions like VPN may require turning off the SPI feature.

MTU Size: The default MTU size is usually fine. 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:

Under MTU Size, enter a new size between 64 and 1500. Then, click Apply to save the new configuration.

Connect Automatically, as Required: Normally, this option should be Enabled, so that an Internet connection will be made automatically, whenever Internet-bound traffic is detected. In locations where Internet access is billed by the minute, if this causes high connection costs, you can disable this setting.

If disabled, you must connect manually, using the sub-screen accessed from the Router Status menu, Connection Status screen.

Configuring 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.

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

- LAN IP addresses—192.168.1.1
- Subnet mask—255.255.255.0

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

From the main menu of the browser interface, under Advanced, click LAN IP Setup to view the menu shown below.

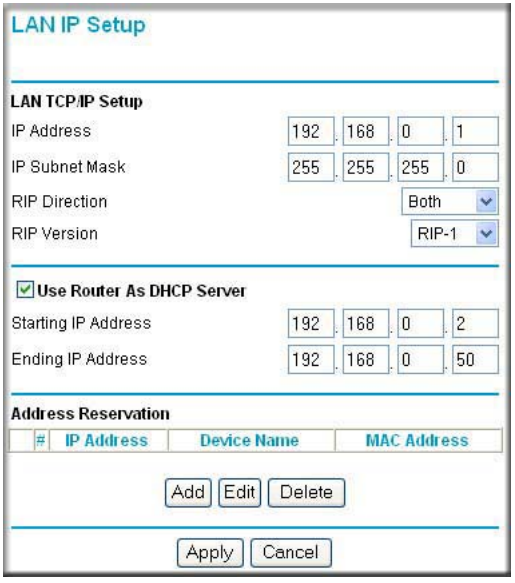


Figure 7-4: LAN IP Setup Menu

The LAN IP parameters are:

IP Address: This is the LAN IP address of the router.

IP Subnet Mask: This is the LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

RIP Direction: RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. Both is the default.

- When set to Both or Out Only, the router 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, it will not send any RIP packets and will ignore any RIP packets received.

RIP Version: This controls the format and the broadcasting method of the RIP packets that the router sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.

- RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
- RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
  - RIP-2B uses subnet broadcasting.
  - RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines because they do not listen to the RIP multicast address and will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting.

Note: If you change the LAN IP address of the router while connected through the browser, you will be disconnected. 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 PCs 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 “IP Configuration by DHCP” on page B-10 for an explanation of DHCP and information about how to assign IP addresses for your network.

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

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

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

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

Using Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC always receives 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. Click the Add button.
2. In the IP Address box, type the IP address to assign to the PC 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 PC or server.

   Tip: If the PC is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.
4. Click Apply to enter the reserved address into the table.

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

To edit or delete a reserved address entry:

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

Using a Dynamic DNS Service

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service 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.

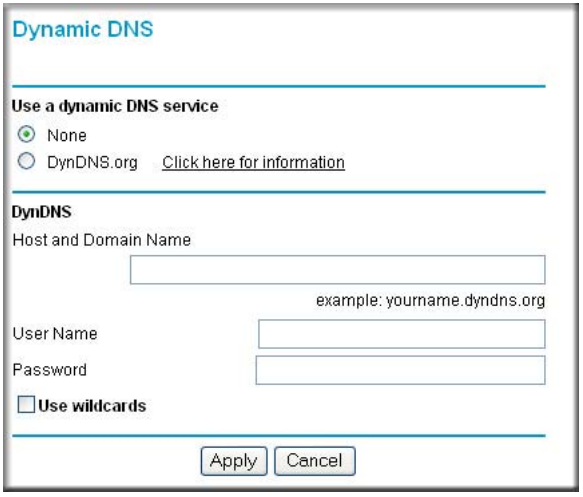


Figure 7-5: Dynamic DNS menu

To configure Dynamic DNS:

1. Register for an account with DynDNS.org. Select “Click here for information” to go to *www.dyndns.org*.
2. Select DynDNS.org.
3. Type the Host Name appended with dyndns.org. For example:

   ```
   myHostName.dyndns.org
   ```

4. Type the User Name for your dynamic DNS account.
5. Type the Password (or key) for your dynamic DNS account.
6. If you want to allow the use of wildcards in resolving your URL, you can select the Use wildcards check box to activate this feature. For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
7. Click Apply to save your configuration.

Configuring Static Routes

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

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

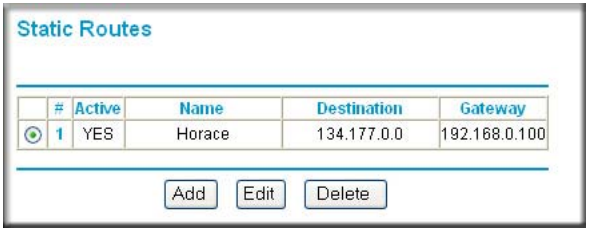


Figure 7-6. Static Routes menu

To add or edit a Static Route:

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

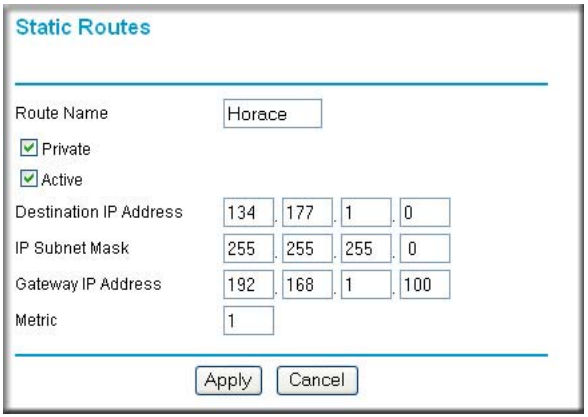


Figure 7-7. Static Route Add/Edit menu

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

Static Route Example

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 134.177.1.0.

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 134.177.1.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.1.0 should be accessed through the ISDN router at 192.168.1.100. The static route would look like Figure 7-7.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.1.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 WGU624 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.

To configure your router for Remote Management:

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

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

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

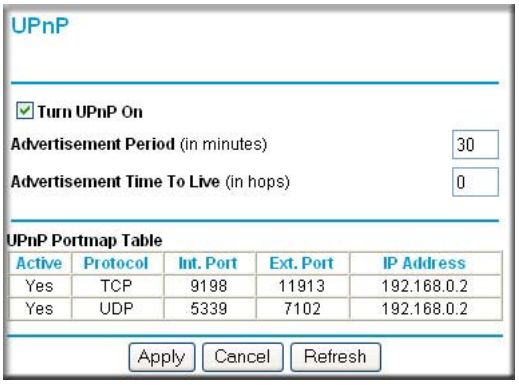


Figure 7-8. UPnP Menu

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 Double 108 Mbps Wireless Firewall Router WGU624. After each problem description, instructions are provided to help you diagnose and solve the problem.

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/WGU624.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 A port LED is lit.
   c. The Wireless G port LED is lit.
   d. The Internet port LED is lit.

If any of these conditions does not occur, refer to 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 800mA 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 sets the router's IP address to 192.168.1.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 8-7.

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 PC on your local network, check the following:

- Check the Ethernet connection between the PC and the router as described in the previous section.
- Make sure your PC's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.1.2 to 192.168.1.254. Refer to "Verifying TCP/IP Properties" on page C-6 or "Verifying TCP/IP Properties for Macintosh Computers" on page C-17 to find your PC's IP address. Follow the instructions in Appendix C to configure your PC.

  Note: If your PC's IP address is shown as 169.254.x.x, recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the router and reboot your PC.
- 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 the Apply button before moving to another menu or tab, or your changes will be lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

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

To check the WAN IP address:

1. Launch your browser and select an external site such as *http://ww.netgear.com*.
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 synchronization 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 PC's host name.
  Assign the PC 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 PC'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 PC's MAC address. This can be done in the Basic Settings menu. Refer to "How to Manually Configure Your Internet Connection" on page 3-9.

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

- Your PC 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 PC and verify the DNS address as described in "Verifying TCP/IP Properties" on page C-6. Alternatively, you may configure your PC manually with DNS addresses, as explained in your operating system documentation.

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

  If your PC obtains its information from the router by DHCP, reboot the PC and verify the gateway address as described in "Verifying TCP/IP Properties" on page C-6.

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 PC or workstation.

Testing the LAN Path to the WGU624

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

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

1. From the Windows toolbar, click on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the router, as in this example:

   `ping 192.168.1.1`

3. Click OK.

   You should see a message like this one:

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

If the path is working, you see this message:

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

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

Request timed out

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

- Wrong physical connections
  - — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "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 PC 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 PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC 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 PC has the IP address of your router listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in "Verifying TCP/IP Properties" on page C-6.

— Check to see that the network address of your PC (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 PC, 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 PCs. 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 PC connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC. Refer to "How to Manually Configure Your Internet Connection" on page 3-9.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the WGU624'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 6-8).
- 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. See "The Router's Rear Panel" on page 2-8 for a picture of the button.

1. Press and hold the default reset button until the Test LED turns on (about 10 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 WGU624 wireless router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.

- Time is off by one hour. Cause: The router does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked “Adjust for Daylight Savings Time”.

Why Does the WGU624 Not Reach Full 108 Mbps Speeds?

Super G complies with IEEE 802.11 a/b/g standards. Because this technology is on the cutting edge, only some combinations of hardware and firmware support full speeds.

- Super G only works in wireless channel 6.
- Super G routers are set to take 54 Mbps or 108 Mbps adapters (called Auto 108 mode), or just 108 Mbps adapters (called 108 Only mode). If 108 Only mode is set, 54 Mbps adapters will not connect.

To get maximum speeds:

1. Upgrade to the latest firmware. The Super G technology is actively being improved, so it's important to keep up-to-date.
2. Use NETGEAR products. Compatibility with non-NETGEAR products is not guaranteed.
3. Only use Super G routers and adapters in your network. Non-Super G devices may slow part or all of your network to lower speed. If the Smart Configuration Utility status line reads 54 Mbps, your devices are probably operating as a standard 802.11g network.
4. Super G is also affected by factors that limit wireless networks in general. For information about optimizing a wireless network, see Chapter 4, “Wireless Configuration”.

Appendix A
Technical Specifications

This appendix provides technical specifications for the Double 108 Mbps Wireless Firewall Router WGU624.

Network Protocol and Standards Compatibility

Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)

Power Adapter

North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	5V DC @ 2.8A output

Physical Specifications

Dimensions:	28 x 175 x 119 mm (1.1 x 6.89 x 4.68 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 EN 55 022 (CISPR 22), Class B C-Tick N10947
Interface Specifications	The router incorporates Auto Uplink™ technology which eliminates the need for crossover cables.
LAN:	10BASE-T or 100BASE-Tx, RJ-45, autosensing and capable of full-duplex or half-duplex operation
WAN:	10BASE-T or 100BASE-Tx, RJ-45, autosensing and capable of full-duplex or half-duplex operation
Wireless	
Radio Data Rates:	1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps Auto Rate Sensing
Frequency:	2.4/5.0 GHz
Data Encoding:	802.11b/g 2.4 GHz to 2.5 GHz CCK and OFDM Modulation 802.11a * 5.15~5.25 GHz (lower band) * 5.25~5.35 GHz (middle band) * 5.725~5.825 GHz (hi-band)
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically up to 30 nodes.
Operating Frequency Ranges:	2.412~2.462 GHz (US) 2.412~2.484 GHz (Japan) 2.412~2.472 GHz (Europe ETSI) 2.457~2.462 GHz (Spain) 2.457~2.472 GHz (France)
Encryption:	40-bit (also called 64-bit), 128-bit, and 152-bit WEP data encryption, WPA encryption

Appendix B
Network, Routing, Firewall, and Basics

This chapter provides an overview of IP networks, routing, and networking.

Related Publications

As you read this document, you may be directed to various Request For Comment (RFC) documents for further information. An RFC is a document published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *http://ww.ietf.org* and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The Double 108 Mbps Wireless Firewall Router WGU624 is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The WGU624 wireless router supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at *http://ww.iana.org*.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The following figure shows the three main address classes, including network and host sections of the address for each address type.

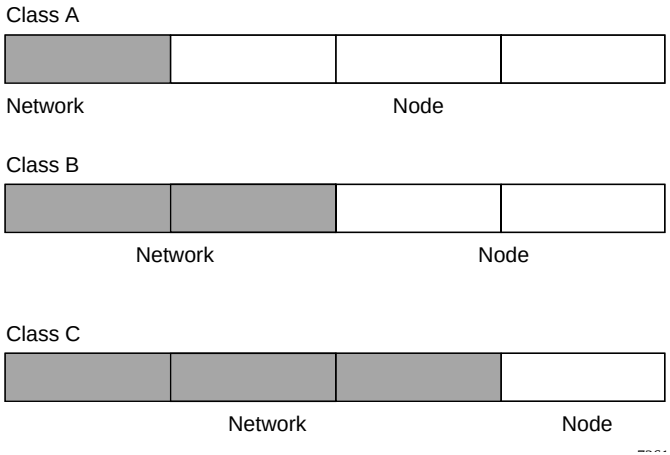


Figure B-1: Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  `1.x.x.x to 126.x.x.x.`

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  `128.1.x.x to 191.254.x.x.`

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  `192.0.1.x to 223.255.254.x.`

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  ```
  224.0.0.0 to 239.255.255.255.
  ```

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

Figure B-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

Note: The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table B-1. Netmask Notation Translation Table for One Octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table B-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29

Table B-2. Netmask Formats

255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

Configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Choose your private network number from this range. The DHCP server of the WGU624 wireless router is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at *http://www.ietf.org*.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The WGU624 wireless router employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.

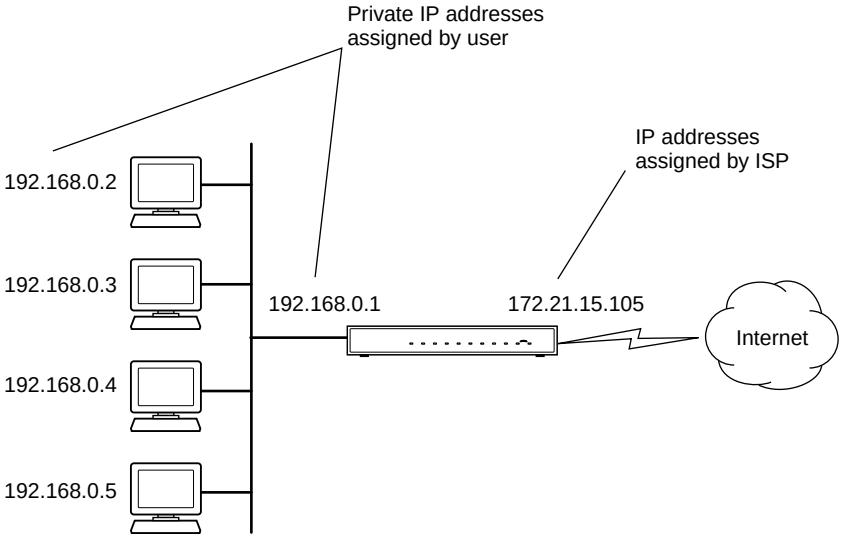


Figure B-3: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The WGU624 wireless router has the capacity to act as a DHCP server.

The WGU624 wireless router also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the process, the network behind the router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection states. Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Ethernet Cabling

Most Ethernet networks now use unshielded twisted pair (UTP) cabling. UTP cable has eight wires arranged in four twisted pairs, and terminated with an RJ45 connector. Normal straight-through UTP Ethernet cable follows the EIA568B standard as described in the table below.

Table B-3. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Category 5 Cable Quality

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

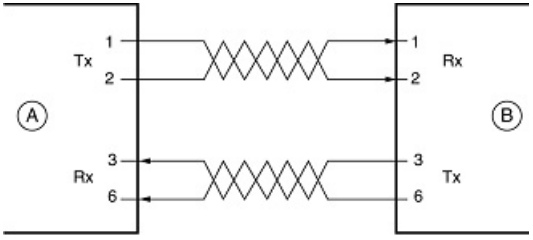
The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Inside Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

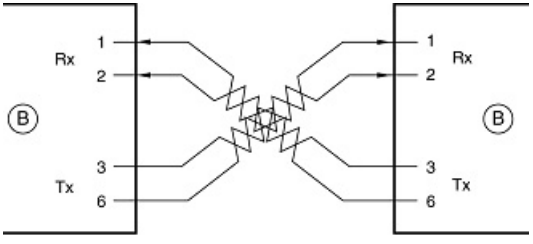
The figure below illustrates straight-through twisted pair cable.



Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-4: Straight-Through Twisted-Pair Cable

The figure below illustrates crossover twisted pair cable.



Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-5: Crossover Twisted-Pair Cable

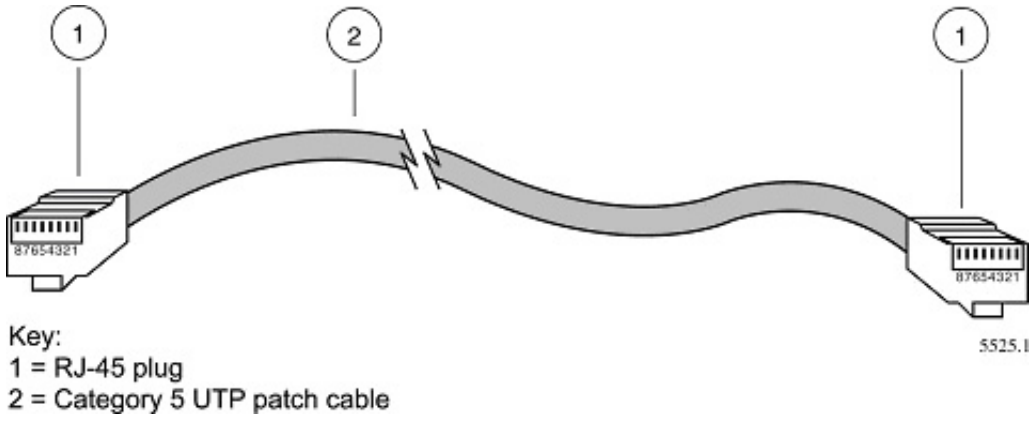


Figure B-6: Category 5 UTP Cable with Male RJ-45 Plug at Each End

Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

The WGU624 wireless router incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, 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.

Appendix C
Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the Double 108 Mbps Wireless Firewall Router WGU624 and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

Note: If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to "Obtaining ISP Configuration Information for Windows Computers" on page C-19 or "Obtaining ISP Configuration Information for Macintosh Computers" on page C-20 for further information.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/ IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/ IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.
- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each PC and the firewall must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to "Appendix B, "Network, Routing, Firewall, and Basics."

The WGU624 wireless router is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.1.2 through 192.168.1.254
- Subnet mask—255.255.255.0
- Gateway address (the firewall)—192.168.1.1

These addresses are part of the IETF-designated private address range for use in private networks.

Configuring Windows 95, 98, and Me for TCP/IP Networking

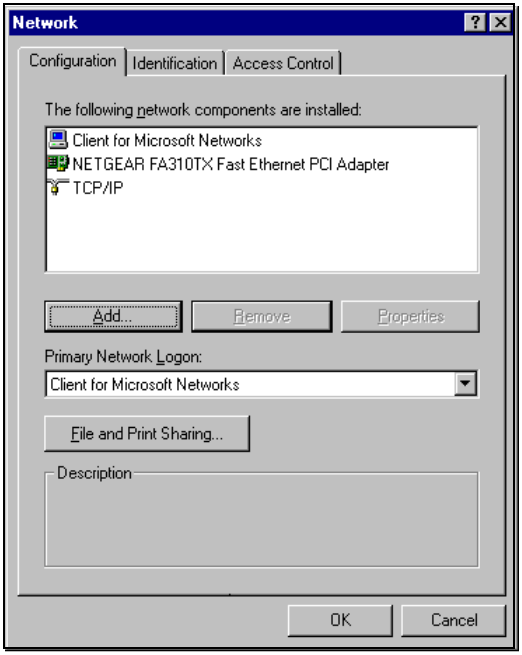
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:



You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

Note: It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

a. Click the Add button.

b. Select Adapter, and then click Add.

c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

a. Click the Add button.

b. Select Protocol, and then click Add.

c. Select Microsoft.

d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

a. Click the Add button.

b. Select Client, and then click Add.

c. Select Microsoft.

d. Select Client for Microsoft Networks, and then click OK.

3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

1

Locate your Network Neighborhood icon.

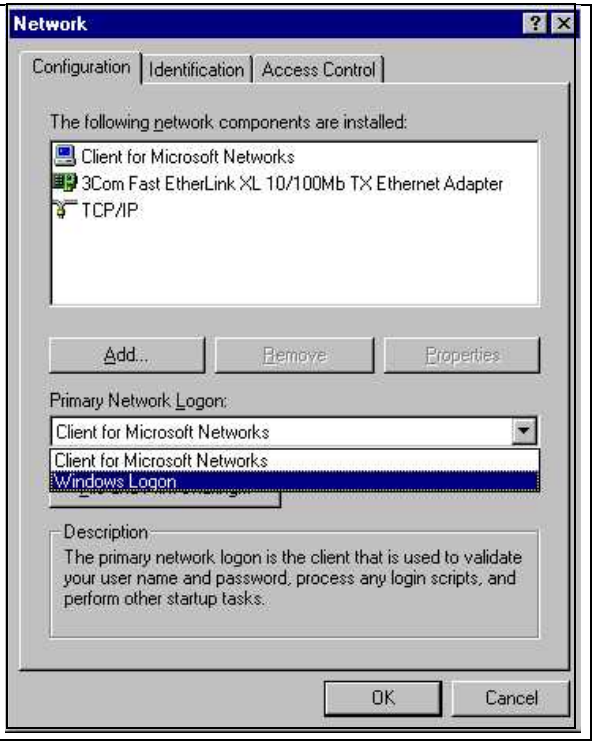
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click Start on the task bar located at the bottom left of the window.
  - Choose Settings, and then Control Panel.
  - Locate the Network Neighborhood icon and click on it. This will open the Network panel as shown below.

2

Verify the following settings as shown:

- Client for Microsoft Network exists
- Ethernet adapter is present
- TCP/IP is present
- Primary Network Logon is set to Windows logon

Click the Properties button. The following TCP/IP Properties window will display.



3

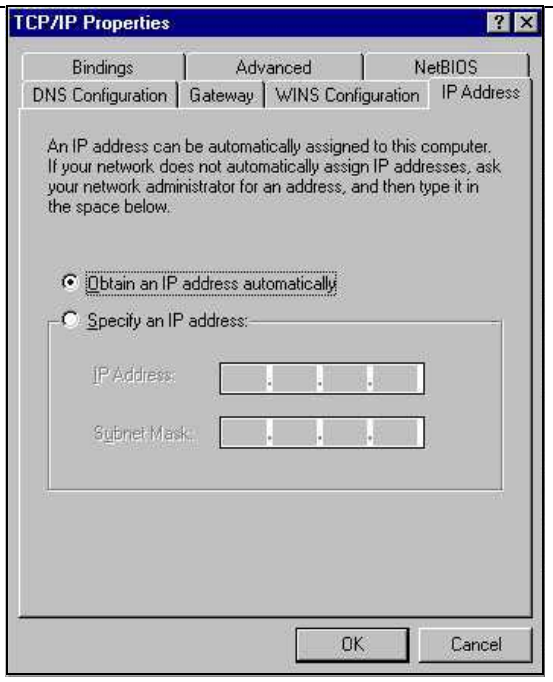
- By default, the IP Address tab is open on this window.
- Verify the following:

  Obtain an IP address automatically is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.

- Click OK to continue.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.
4. Select "I want to connect through a Local Area Network" and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.

2. Type **winipcfg**, and then click OK.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.1.2 and 192.168.1.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.1.1

Configuring Windows NT4, 2000 or XP for IP Networking

As part of the PC preparation process, you may need to install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.
6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Then, restart your PC.

DHCP Configuration of TCP/IP in Windows XP, 2000, or NT4

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

DHCP Configuration of TCP/IP in Windows XP

1

Locate your Network Neighborhood icon.

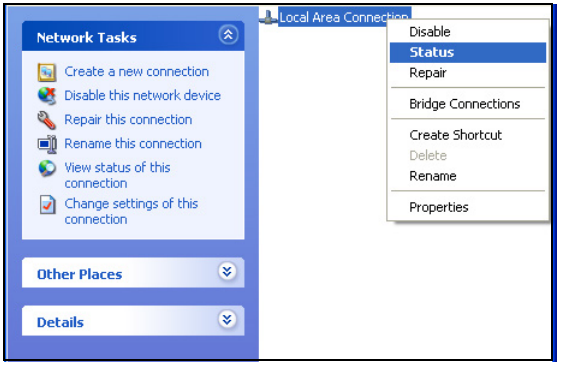
- Select Control Panel from the Windows XP new Start Menu.
- Select the Network Connections icon on the Control Panel. This will take you to the next step.

2

- Now the Network Connection window displays.

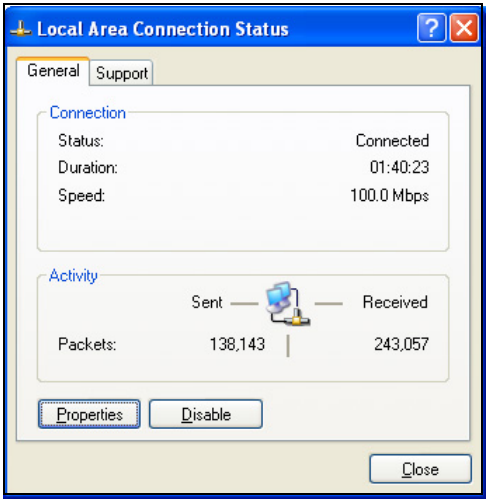
  The Connections List that shows all the network connections set up on the PC, located to the right of the window.

- Right-click on the Connection you will use and choose Status.



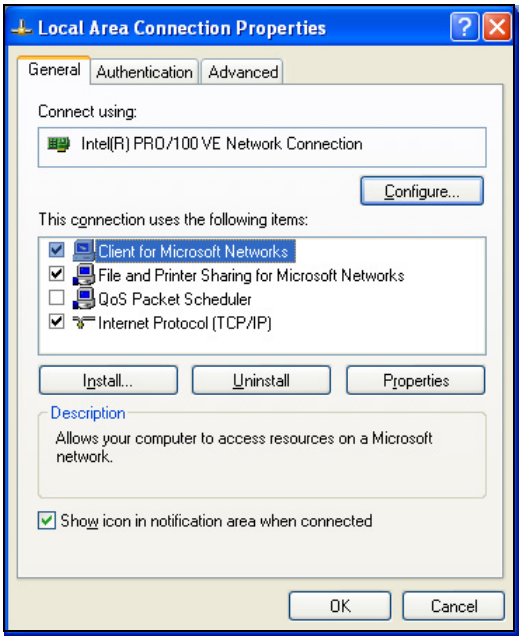
3

- Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.
- Administrator logon access rights are needed to use this window.
- Click the Properties button to view details about the connection.



4

- The TCP/IP details are presented on the Support tab page.
- Select Internet Protocol**,** and click Properties to view the configuration information**.**

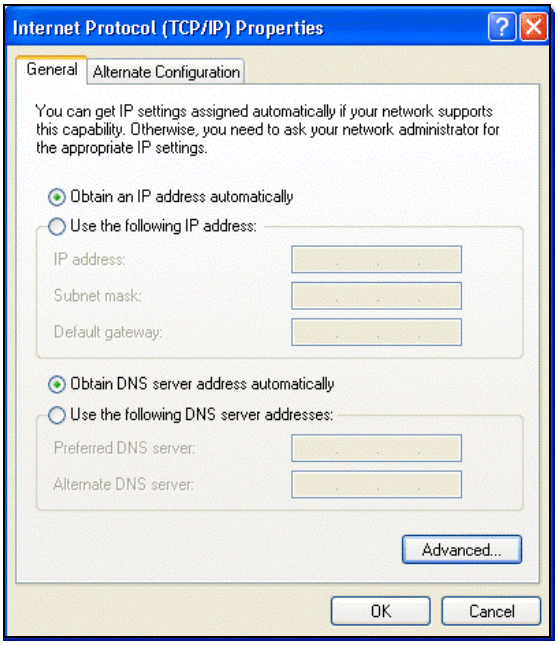


5

- Verify that the Obtain an IP address automatically radio button is selected.
- Verify that Obtain DNS server address automatically radio button is selected.
- Click the OK button.

This completes the DHCP configuration of TCP/IP in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.



DHCP Configuration of TCP/IP in Windows 2000

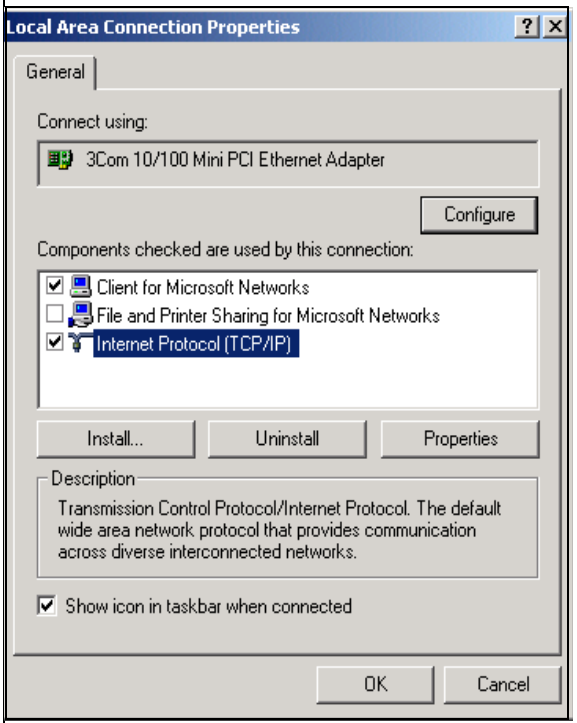
Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

1

- Click on the My Network Places icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.
- Right click on Local Area Connection and select Properties.

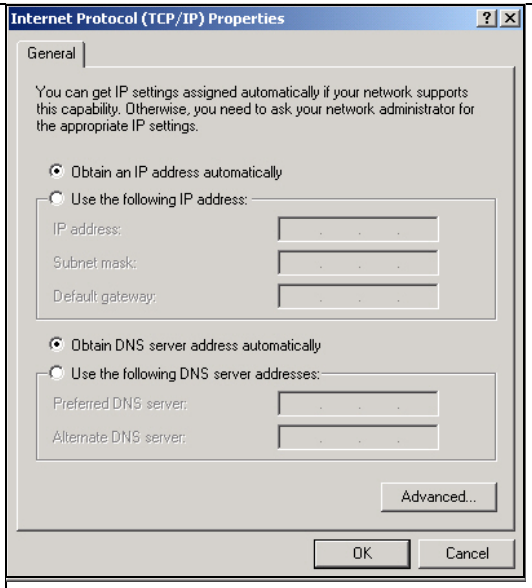
2

- The Local Area Connection Properties dialog box appears.
- Verify that you have the correct Ethernet card selected in the Connect using box.
- Verify that at least the following two items are displayed and selected in the box of "Components checked are used by this connection:"
  - Client for Microsoft Networks and
  - Internet Protocol (TCP/IP)
- Click OK.



3

- With Internet Protocol (TCP/IP) selected, click Properties to open the Internet Protocol (TCP/IP) Properties dialogue box.
- Verify that
  - Obtain an IP address automatically is selected.
  - Obtain DNS server address automatically is selected.
- Click OK to return to Local Area Connection Properties.

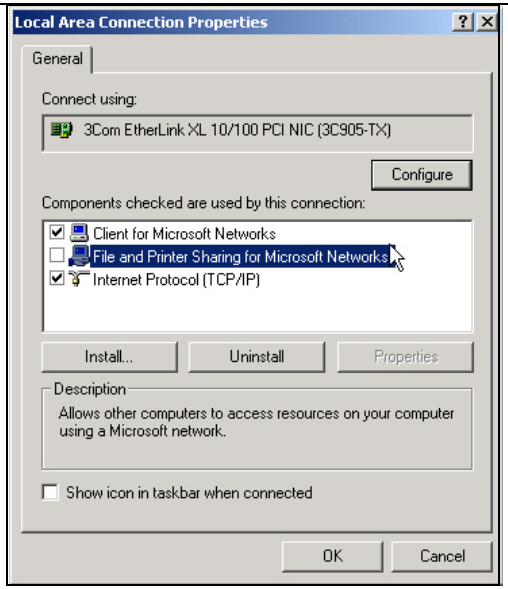


4

- Click OK again to complete the configuration process for Windows 2000.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



DHCP Configuration of TCP/IP in Windows NT4

Once you have installed the network card, you need to configure the TCP/IP environment for Windows NT 4.0. Follow this procedure to configure TCP/IP with DHCP in Windows NT 4.0.

1

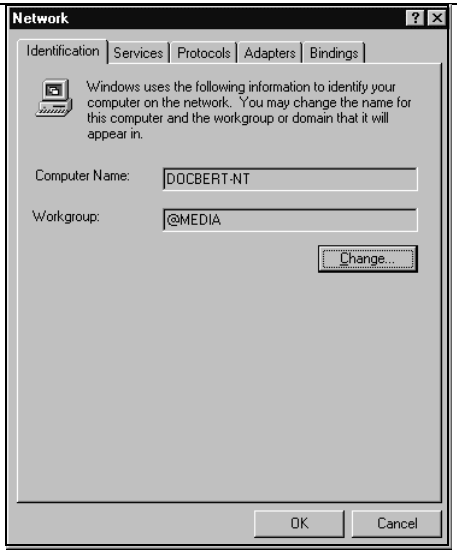
- Choose Settings from the Start Menu, and then select Control Panel. This will display Control Panel window.

2

- Double-click the Network icon in the Control Panel window.

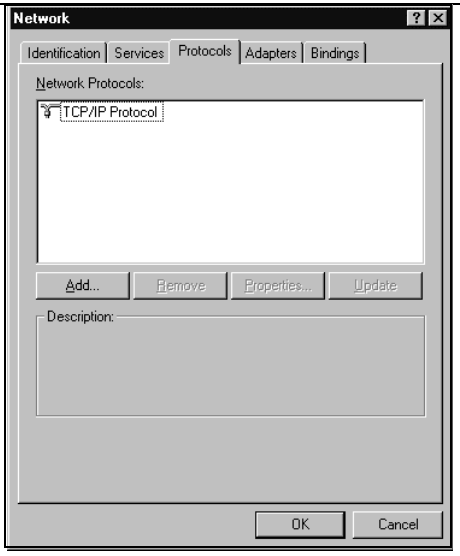
  The Network panel will display.

- Select the Protocols tab to continue.



3

- Highlight the TCP/IP Protocol in the Network Protocols box, and click on the Properties button.

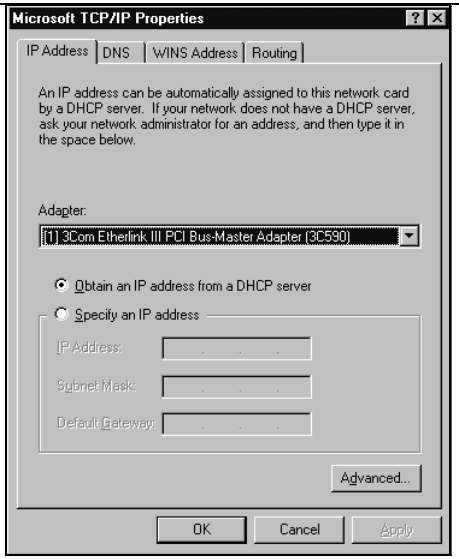


4

- The TCP/IP Properties dialog box now displays.
- Click the IP Address tab**.**
- Select the radio button marked Obtain an IP address from a DHCP server**.**
- Click OK. This completes the configuration of TCP/IP in Windows NT.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

   The Run window opens.

2. Type **`cmd`** and then click OK.

   A command window opens

3. Type **`ipconfig /all`**

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.1.2 and 192.168.1.254.
   - The subnet mask is 255.255.255.0.

- The default gateway is 192.168.1.1.

4. Type **`exit.`**

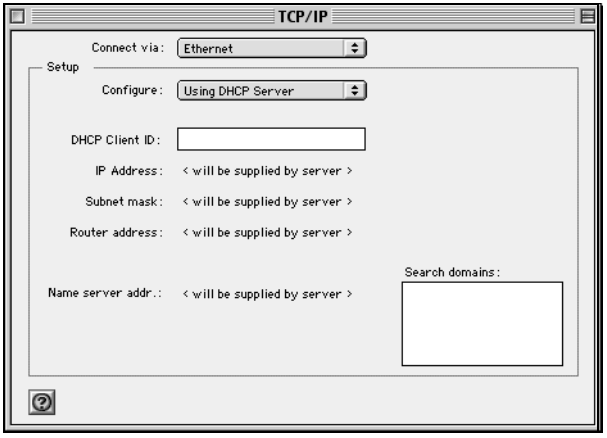
Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens:



2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.

   You can leave the DHCP Client ID box empty.

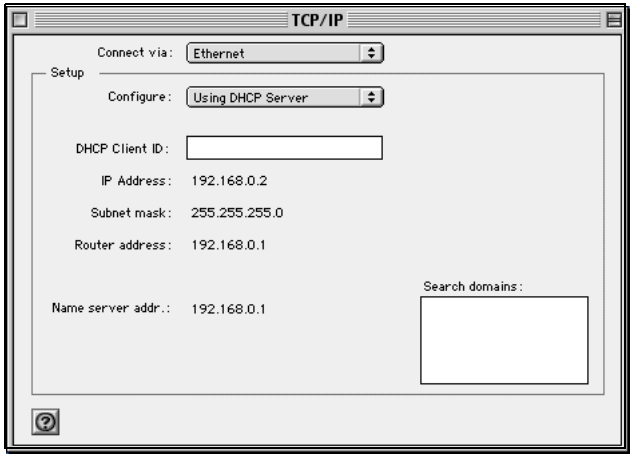
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

MacOS X

1. From the Apple menu, choose System Preferences, then Network.
2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.



The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.1.2 and 192.168.1.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.1.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

Verifying the Readiness of Your Internet Account

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your firewall does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your firewall takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the firewall's Internet port is connected to the broadband modem, the firewall appears to be a single PC to the ISP. The firewall then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the firewall to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you will need to enter your login name and password in the router's configuration menus. After your network and firewall are configured, the firewall will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

  For example, your account's full server names may look like this:

  `mail.xxx.yyy.com`

  In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your firewall automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the firewall. These procedures are described next.

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the WGU624 wireless router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components.
3. Select TCP/IP, and then click Properties.

   The TCP/IP Properties dialog box opens.
4. Select the IP Address tab.

   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".
5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

   If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

   You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the WGU624 wireless router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the "Configure" setting to "Using DHCP Server".

7. Close the TCP/IP Control Panel.

Restarting the Network

Once you've set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your WGU624 wireless router, you are ready to access and configure the firewall.

Appendix D
Wireless Networking Basics

This chapter provides an overview of Wireless networking.

Wireless Networking Overview

The WGU624 wireless router conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard for wireless LANs (WLANs) and a product update will bring the WGU624 into conformance to the 802.11g standard when it is ratified. On an 802.11b or g wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected. The 802.11g auto rate sensing rates are 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see *http://www.wi-fi.net*), an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network — ad hoc and infrastructure.

Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

Ad Hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network — each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as peer-to-peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Network Name: Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

Authentication and WEP

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is used when the wireless devices are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

802.11 Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point such as the one built in to the WGU624:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.

- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated in below.

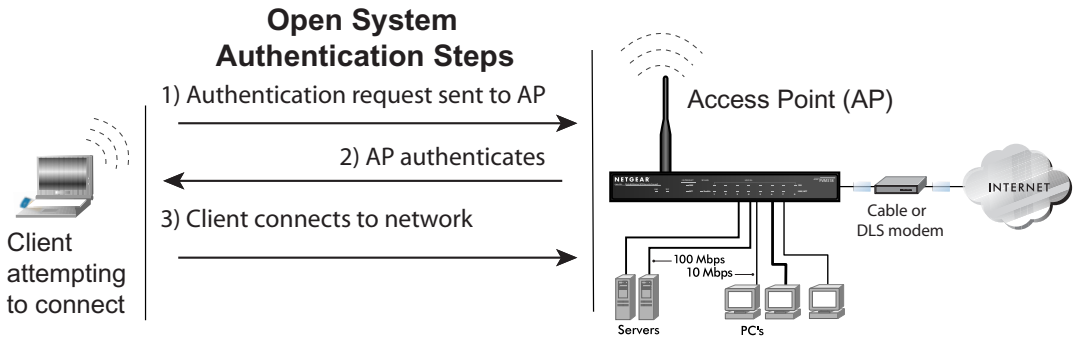


Figure 6-1: Open system authentication

Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.
3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.

5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

This process is illustrated in below.

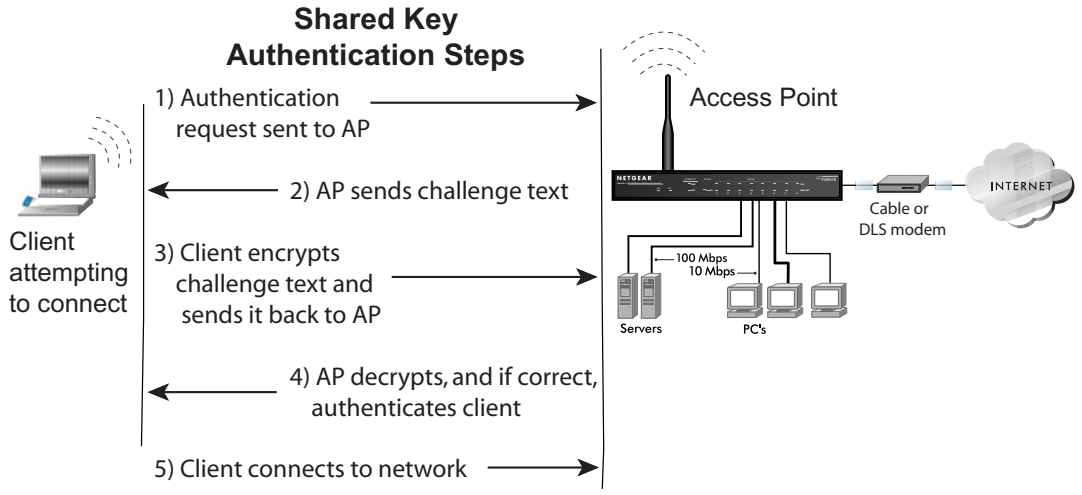


Figure 6-2: Shared key authentication

Overview of WEP Parameters

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. **Use WEP for Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the wireless network uses Open System Authentication.

3. **Use WEP for Authentication and Encryption:** A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving 802.11 device decrypts the data using the same WEP Key. For authentication purposes, the 802.11 network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption).

Key Size

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90” is a 40-bit WEP Key.

When configured for 128-bit encryption, wireless products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

Note: Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters configurations match.

WEP Configuration Options

The WEP settings must match on all 802.11 devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11 access points and all of the 802.11 client adapters on the network must have the same WEP settings.

Note: Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP's WEP key 2 is the same as the client's WEP key 2 and the AP's WEP key 3 is the same as the client's WEP key 3.

Wireless Channels

IEEE 802.11 wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel crosstalk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in Table 6-1:

Table 6-1. 802.11 Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

Note: The available channels supported by the wireless products in various countries are different.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

WPA Wireless Security

Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

The IEEE introduced the WEP as an optional security measure to secure 802.11b (Wi-Fi) WLANs, but inherent weaknesses in the standard soon became obvious. In response to this situation, the Wi-Fi Alliance announced a new security architecture in October 2002 that remedies the shortcomings of WEP. This standard, formerly known as Safe Secure Network (SSN), is designed to work with existing 802.11 products and offers forward compatibility with 802.11i, the new wireless security architecture being defined in the IEEE.

WPA offers the following benefits:

- Enhanced data privacy
- Robust key management
- Data origin authentication
- Data integrity protection

How Does WPA Compare to WEP?

WEP is a data encryption method and is not intended as a user authentication mechanism. WPA user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Support for 802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional. For details on EAP specifically, refer to IETF's RFC 2284.

With 802.11 WEP, all access points and client wireless adapters on a particular wireless LAN must use the same encryption key. A major problem with the 802.11 standard is that the keys are cumbersome to change. If you do not update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. Products based on the 802.11 standard alone offer system administrators no effective method to update the keys.

For 802.11, WEP encryption is optional. For WPA, encryption using Temporal Key Integrity Protocol (TKIP) is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of known WEP vulnerabilities.

How Does WPA Compare to IEEE 802.11i?

WPA will be forward compatible with the IEEE 802.11i security specification currently under development. WPA is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in WPA are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols, such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

What are the Key Features of WPA Security?

The following security features are included in the WPA standard:

- WPA Authentication
- WPA Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael message integrity code (MIC)
  - AES Support (to be phased in)
- Support for a Mixture of WPA and WEP Wireless Clients, but mixing WEP and WPA is discouraged

These features are discussed below.

WPA addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks as found in the enterprise. This infrastructure includes stations, access points, and authentication servers (typically RADIUS servers). The RADIUS server holds (or has access to) user credentials (for example, user names and passwords) and authenticates wireless users before they gain access to the network.

The strength of WPA comes from an integrated sequence of operations that encompass 802.1X/ EAP authentication and sophisticated key management and encryption techniques. Its major operations include:

- Network security capability determination. This occurs at the 802.11 level and is communicated through WPA information elements in Beacon, Probe Response, and (Re) Association Requests. Information in these elements includes the authentication method (802.1X or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES).

The primary information conveyed in the Beacon frames is the authentication method and the cipher suite. Possible authentication methods include 802.1X and Pre-shared key. Pre-shared key is an authentication method that uses a statically configured pass phrase on both the stations and the access point. This obviates the need for an authentication server, which in many home and small office environments will not be available nor desirable. Possible cipher suites include: WEP, TKIP, and AES (Advanced Encryption Standard). We talk more about TKIP and AES when addressing data privacy below.

- Authentication. EAP over 802.1X is used for authentication. Mutual authentication is gained by choosing an EAP type supporting this feature and is required by WPA. 802.1X port access control prevents full access to the network until authentication completes. 802.1X EAPOL-Key packets are used by WPA to distribute per-session keys to those stations successfully authenticated.

  The supplicant in the station uses the authentication and cipher suite information contained in the information elements to decide which authentication method and cipher suite to use. For example, if the access point is using the pre-shared key method then the supplicant need not authenticate using full-blown 802.1X. Rather, the supplicant must simply prove to the access point that it is in possession of the pre-shared key. If the supplicant detects that the service set does not contain a WPA information element then it knows it must use pre-WPA 802.1X authentication and key management in order to access the network.

- Key management. WPA features a robust key generation/management system that integrates the authentication and data privacy functions. Keys are generated after successful authentication and through a subsequent 4-way handshake between the station and Access Point (AP).

- Data Privacy (Encryption). Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.

- Data integrity. TKIP includes a message integrity code (MIC) at the end of each plaintext message to ensure messages are not being spoofed.

WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

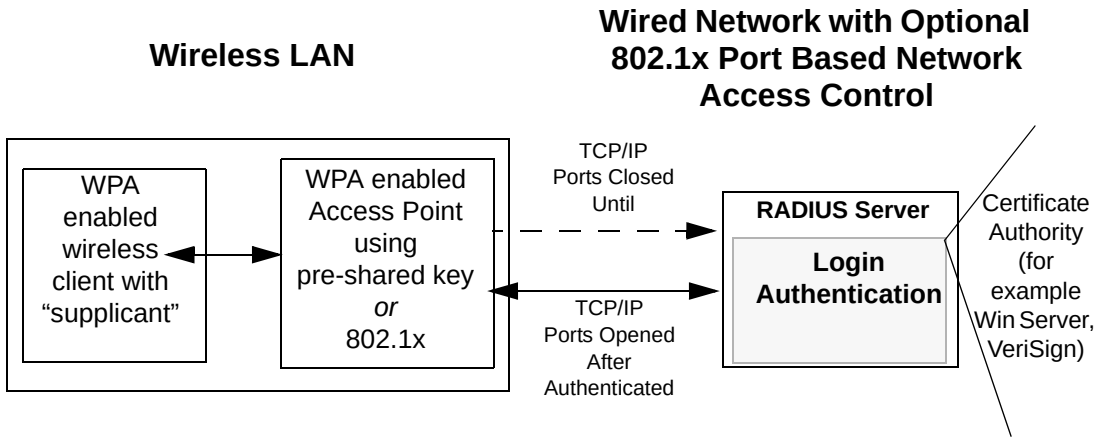


Figure D-1: WPA Overview

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as providing a vehicle for dynamically varying data encryption keys via EAP from a RADIUS server, for example. This framework enables using a central authentication server, which employs mutual authentication so that a rogue wireless user does not join the network.

It is important to note that 802.1x does not provide the actual authentication mechanisms. When using 802.1x, the EAP type, such as Transport Layer Security (EAP-TLS), or EAP Tunneled Transport Layer Security (EAP-TTLS), defines how the authentication takes place.

Note: For environments with a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports Extensible Authentication Protocol (EAP). For environments without a RADIUS infrastructure, WPA supports the use of a pre-shared key.

Together, these technologies provide a framework for strong user authentication.

Windows XP implements 802.1x natively, and several NETGEAR switch and wireless access point products support 802.1x.

Client with a WPA-enabled wireless adapter and supplicant (Win XP, Funk, Meetinghouse)	For example, a WPA-enabled AP	For example, a RADIUS server

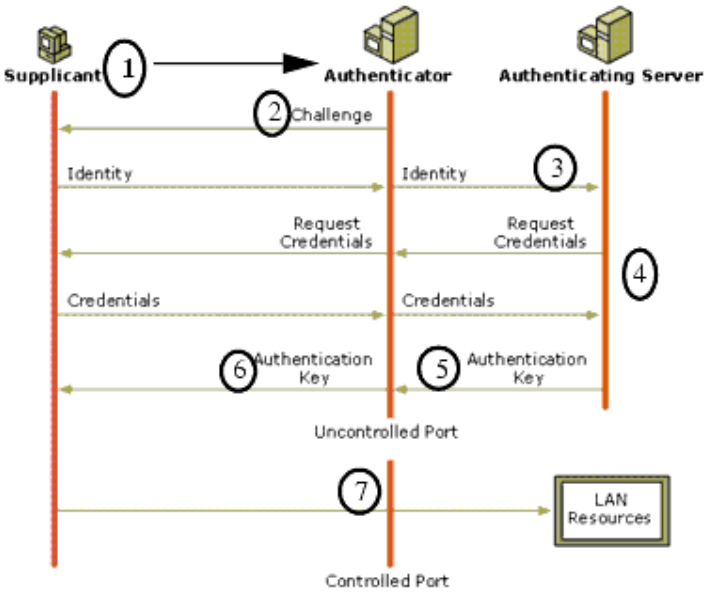


Figure D-2: 802.1x Authentication Sequence

The AP sends Beacon Frames with WPA information element to the stations in the service set. Information elements include the required authentication method (802.1x or Pre-shared key) and the preferred cipher suite (WEP, TKIP, or AES). Probe Responses (AP to station) and Association Requests (station to AP) also contain WPA information elements.

1. Initial 802.1x communications begin with an unauthenticated supplicant (client device) attempting to connect with an authenticator (802.11 access point). The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.

3. The client sends an EAP-response packet containing the identity to the authentication server. The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (for example, RADIUS).
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or some other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application “supplicant” software on the client devices. The access point acts as a “pass through” for 802.1x messages, which means that you can specify any EAP type without needing to upgrade an 802.1x-compliant access point. As a result, you can update the EAP authentication type to such devices as token cards (Smart Cards), Kerberos, one-time passwords, certificates, and public key authentication, or as newer types become available and your requirements for security change.

WPA Data Encryption Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required.

For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility (the Information Element) for the wireless AP to advertise the changed key to the connected wireless clients.

If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

Temporal Key Integrity Protocol (TKIP)

WPA uses TKIP to provide important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte message integrity check (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

Optional AES Support to be Phased In

One of the encryption methods supported by WPA, besides TKIP, is the advanced encryption standard (AES), although AES support will not be required initially for Wi-Fi certification. This is viewed as the optimal choice for security conscience organizations, but the problem with AES is that it requires a fundamental redesign of the NIC's hardware in both the station and the access point. TKIP is a pragmatic compromise that allows organizations to deploy better security while AES capable equipment is being designed, manufactured, and incrementally deployed.

Is WPA Perfect?

WPA is not without its vulnerabilities. Specifically, it is susceptible to denial of service (DoS) attacks. If the access point receives two data packets that fail the message integrity code (MIC) within 60 seconds of each other, then the network is under an active attack, and as a result, the access point employs counter measures, which include disassociating each station using the access point. This prevents an attacker from gleaning information about the encryption key and alerts administrators, but it also causes users to lose network connectivity for 60 seconds. More than anything else, this may just prove that no single security tactic is completely invulnerable. WPA is a definite step forward in WLAN security over WEP and has to be thought of as a single part of an end-to-end network security strategy.

Product Support for WPA

Starting in August, 2003, NETGEAR, Inc. wireless Wi-Fi certified products will support the WPA standard. NETGEAR, Inc. wireless products that had their Wi-Fi certification approved before August, 2003 will have one year to add WPA so as to maintain their Wi-Fi certification.

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

Supporting a Mixture of WPA and WEP Wireless Clients is Discouraged

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

However, a mixed mode supporting WPA and non-WPA clients would offer network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged.

Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**
  To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

Changes to Wireless Network Adapters

Wireless networking software in the adapter, and possibly in the OS or client application, must be updated to support the following:

- **The new WPA information element**
  Wireless clients must be able to process the WPA information element and respond with a specific security configuration.
- **The WPA two-phase authentication**
  Open system, then 802.1x supplicant (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update your Microsoft Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA authentication (and preshared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

To obtain the Microsoft WPA client program, visit the Microsoft Web site.

Glossary

Use the list below to find definitions for technical terms used in this manual.

List of Glossary Terms

10BASE-T
IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx
IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

3DES
3DES (Triple DES) achieves a high level of security by encrypting the data three times using DES with three different, unrelated keys.

802.1x
802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management.
The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

802.11a
IEEE specification for wireless networking at 54 Mbps operating in unlicensed radio bands over 5 GHz.

802.11b
IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5 GHz.

802.11g
A soon to be ratified IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5 GHz. 802.11g is backwards compatible with 802.11b.

ADSL

Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

AES

Advanced Encryption Standard, a symmetric 128-bit block data encryption technique.
It is an iterated block cipher with a variable block length and a variable key length. The block length and the key length can be independently specified to 128, 192 or 256 bits.The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

AH

Authentication Header.

ARP

Address Resolution Protocol, a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address.
A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

Auto Uplink

Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

CA

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

Cat 5

Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA).
This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Certificate Authority

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.
The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

CRL
Certificate Revocation List. Each Certificate Authority (CA) maintains a revoked certificates list.

Denial of Service attack
DoS. A hacker attack designed to prevent your computer or network from operating or communicating.

DHCP
An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

DMZ
A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network.
The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DNS
Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.
Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name
A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DoS
A hacker attack designed to prevent your computer or network from operating or communicating.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSLAM

DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

Dynamic Host Configuration Protocol

DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

EAP

Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods.
EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

ESP

Encapsulating Security Payload.

ESSID

The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Gateway

A local device, usually a router, that connects hosts on a local network to other networks.

IETF

Internet Engineering Task Force. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at *www.ietf.org*.
An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

IKE
Internet Key Exchange. An automated method for exchanging and managing encryption keys between two VPN devices.

IP
Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address
A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
Ranges of addresses are assigned by Internic, an organization formed for this purpose.

IPSec
Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.

IPX
Short for Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems.
Like UDP/IP, IPX is a datagram protocol used for connectionless communications. Higher-level protocols, such as SPX and NCP, are used for additional error recovery services.

ISP
Internet service provider.

Internet Protocol
The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

LAN
A communications network serving users within a limited area, such as one floor of a building.

LDAP
A set of protocols for accessing information directories.

Lightweight Directory Access Protocol
LDAP. A set of protocols for accessing information directories.
LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Because it's a simpler version of X.500, LDAP is sometimes called *X.500-lite.*

local area network
LAN. A communications network serving users within a limited area, such as one floor of a building.

A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.

MAC address
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Mbps
Megabits per second.

MD5
MD5 creates digital signatures using a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.
When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been tampered with. This comparison is called a "hashcheck."

MDI/MDIX
In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). See also AES.

Maximum Receive Unit
The size in bytes of the largest packet that can be sent or received.

Maximum Transmit Unit
The size in bytes of the largest packet that can be sent or received.

Most Significant Bit or Most Significant Byte
MSB. The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

MRU
The size in bytes of the largest packet that can be sent or received.

MSB
MSB. The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

MTU
The size in bytes of the largest packet that can be sent or received.

NAT
A technique by which several hosts share a single IP address for access to the Internet.

NetBIOS
The Network Basic Input Output System is an application programming interface (API) for sharing services and information on local-area networks (LANs).
Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, up to 16 characters in length.

Network Address Translation
NAT. A technique by which several hosts share a single IP address for access to the Internet.

NIC
Network Interface Card. An adapter in a computer which provides connectivity to a network.

NID
Network Interface Device. The point of demarcation, where the telephone line comes into the house.

packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Perfect Forward Secrecy
Perfect Forward Secrecy (PFS) provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.

PKIX
PKIX. The most widely used standard for defining digital certificates.

Point-to-Point Protocol
PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPP
A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPPoA
PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPPoE
PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over ATM
PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over Ethernet
PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPTP
Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.

PSTN
Public Switched Telephone Network.

Public Key Infrastructure
PKIX. The most widely used standard for defining digital certificates.
X.509 is actually an ITU Recommendation, which means that it has not yet been officially defined or approved. As a result, companies have implemented the standard in different ways. For example, both Netscape and Microsoft use X.509 certificates to implement SSL in their Web servers and browsers. But an X.509 Certificate generated by Netscape may not be readable by Microsoft products, and vice versa.

RADIUS
Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system.
Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

RFC
Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at *www.ietf.org*.

RIP
A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

Routing Information Protocol
RIP. A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

SSID
A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.
This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Subnet Mask
A mask used to determine what subnet an IP address belongs to. Subnetting enables a network administrator to further divide an IP address into two or more subnets.
An IP address has two components, the network address and the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.
Subnetting enables the network administrator to further divide the host part of the address into two or more subnets. In this case, a part of the host address is reserved to identify the particular subnet. This is easier to see if we show the IP address in binary format. The full address is: 10010110.11010111.00010001.00001001
The Class B network part is: 10010110.11010111
and the host address is 00010001.00001001
If this network is divided into 14 subnets, however, then the first 4 bits of the host address (0001) are reserved for identifying the subnet.

The subnet mask is the network address plus the bits reserved for identifying the subnetwork. (By convention, the bits for the network address are all set to 1, though it would also work if the bits were set exactly as in the network address.) In this case, therefore, the subnet mask would be 11111111.11111111.11110000.00000000. It's called a mask because it can be used to identify the subnet to which an IP address belongs by performing a bitwise AND operation on the mask and the IP address. The result is the subnetwork address: Subnet Mask 255.255.240.000 11111111.11111111.11110000.00000000
IP Address 150.215.017.009 10010110.11010111.00010001.00001001
Subnet Address 150.215.016.000 10010110.11010111.00010000.00000000

The subnet address, therefore, is 150.215.016.000.

TCP/IP
The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

TLS
Short for Transport Layer Security, TLS is a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.

The TLS protocol is made up of two layers. The TLS Record Protocol ensures that a connection is private by using symmetric data encryption and ensures that the connection is reliable. The second TLS layer is the TLS Handshake Protocol, which allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before data is transmitted or received. Based on Netscape's SSL 3.0, TLS supercedes and is an extension of SSL. TLS and SSL are not interoperable.

Universal Plug and Play

UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

VCI

Virtual Channel Identifier. Together with the VPI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.

VPI

Virtual Path Identifier. Together with the VCI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.

VPN

Virtual Private Network. A method for securely transporting data between two private networks by using a public network such as the Internet as a connection.

WAN

A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

WEB Proxy Server

A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall.
The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

WEP

Wired Equivalent Privacy is a data encryption protocol for 802.11b wireless networks.
All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

wide area network
WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

Wi-Fi
A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

Windows Internet Naming Service
WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.
If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS
WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Wireless Network Name (SSID)
Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

W