Reference Manual for the Wireless Router and Voice Adapter WGR613VAL

NETGEAR

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

202-10093-01
March 2005

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

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

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

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

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

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

EN 55 022 Declaration of Conformance

This is to certify that the WGR613VAL Wireless Router and Voice Adapter is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das WGR613VAL Wireless Router and Voice Adapter 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 WGR613VAL Wireless Router and Voice Adapter 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 WGR613VAL Wireless Router and Voice Adapter.

World Wide Web

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

Product and Publication Details

Model Number:	WGR613VAL
Publication Date:	March 2005
Product Family:	router
Product Name:	WGR613VAL Wireless Router and Voice Adapter
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10093-01

Contents

Appendix A
Technical Specifications

Appendix B
Network, Routing, and Firewall Basics

Appendix C
Preparing Your Network

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
`fixed`	Screen text, file and server names, extensions, commands, IP addresses

This guide uses the following formats to highlight special messages:

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

This manual is written for the WGR613VAL wireless router according to these specifications:

Table 1-2. Manual Scope

Product Version	WGR613VAL Wireless Router and Voice Adapter
Manual Publication Date	March 2005

➡	**Note:** Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/WGR613VAL.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print this Manual

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

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

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

- **Printing a Chapter**.

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

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

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

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

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

- **Printing the Full Manual**.

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

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

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

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

Chapter 2
Getting to Know Your NETGEAR Wireless Router

NETGEAR WGR613VAL wireless routers provide connections for multiple computers to the Internet through an external broadband access device such as a cable modem or DSL modem that is normally intended for use by a single computer. This chapter introduces the NETGEAR WGR613VAL Wireless Router and Voice Adapter.

Package Contents

The product package should contain the following items:

- WGR613VAL Wireless Router and Voice Adapter.
- AC power adapter.
- A Category 5 (CAT5) Ethernet cable.
- The Setup CD, including:
  - This guide.
  - Application Notes and other helpful information.
- Support Registration 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 Front Panel

The front of the WGR613VAL wireless router includes these status lights you can use to verify connections.

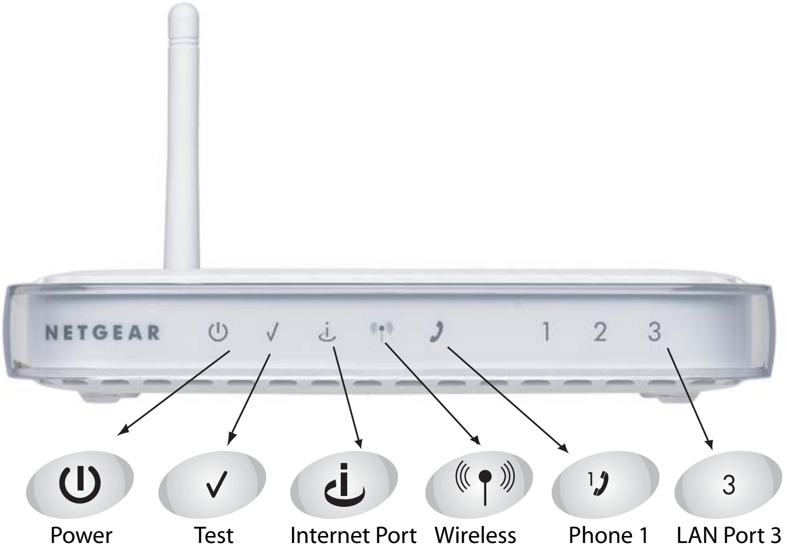


Figure 2-1: WGR613VAL Front Panel

Viewed from left to right, the table below describes the lights on the front panel of the router.

Table 2-1. Status Light Descriptions

Label	Activity	Description
Power	On Green Solid Off	Power is supplied to the router. Power is not supplied to the router.
Test	Blinking Off	The router is performing its diagnostic test. The router successfully completed its diagnostic test.
Internet Port	On Blink	The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
Wireless	On	The 802.11g wireless interface is enabled.

Table 2-1. Status Light Descriptions (continued)

Label	Activity	Description
Phone Port	Off On	The phone port has not yet been provisioned by the service provider. The phone port has been provisioned by the service provider.
LAN Ports	Green Amber	The LAN port has detected a 100 Mbps link with an attached device. The LAN port has detected a 10 Mbps link with an attached device.

The Rear Panel

The rear panel of the WGR613VAL router contains the items listed below.

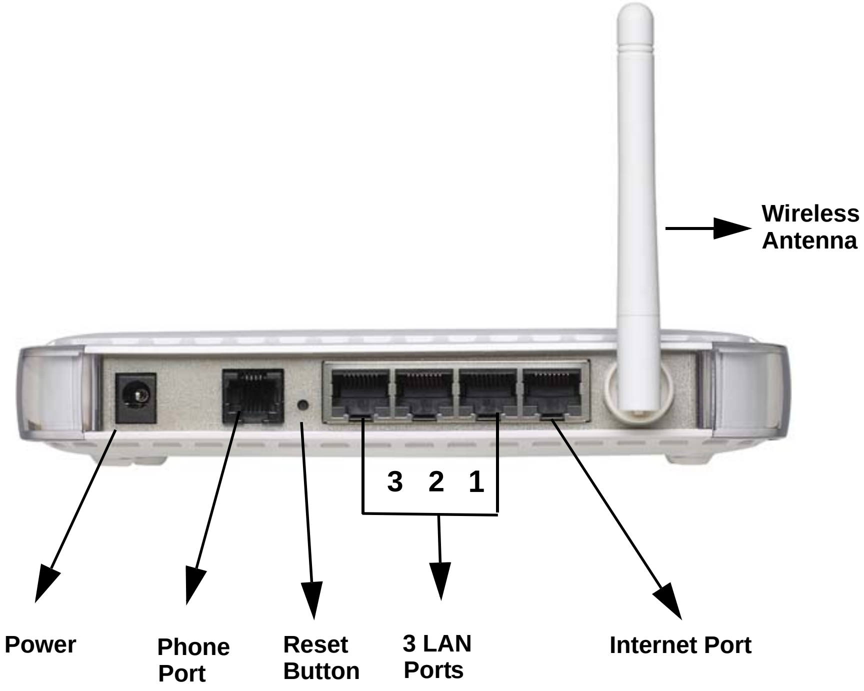


Figure 1-2: WGR613VAL Rear Panel

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

- Outlet for 12V DC @ 1.2A output AC power adapter
- One phone port

- Factory default reset push button for Restoring the Default Configuration and Password
- Three LAN phone ports
- Internet (WAN) Ethernet port for connecting the router to a cable or DSL modem
- 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 wireless router for Internet access.

Follow these instructions to set up your router.

Prepare to Install Your Wireless Router

- *For Cable Modem Service*: When you perform the wireless router setup steps be sure to use the computer you first registered with your cable ISP.
- *For DSL Service*: You may need information such as the DSL login name/e-mail address and password in order to complete the wireless router setup.

Before proceeding with the wireless router installation, familiarize yourself with the contents of the Setup CD, especially this manual and the tutorials for configuring computers for networking.

First, Connect the Wireless Router to Your Network

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

a. Turn off your computer.

b. Turn off the cable or DSL broadband modem.

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

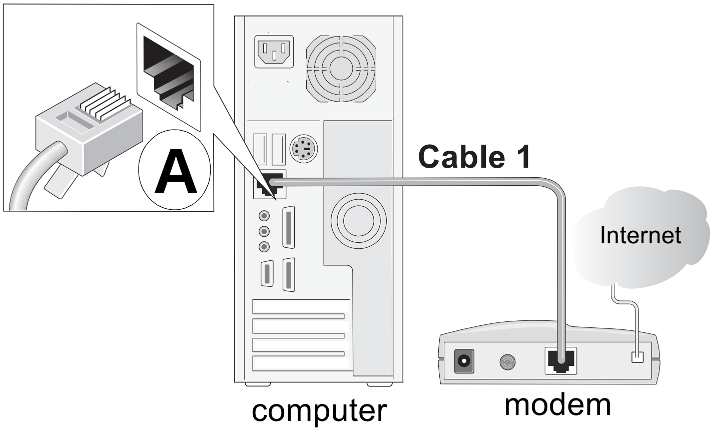


Figure 3-1: Disconnect the Ethernet cable from the computer

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

e. 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** of the diagram below.

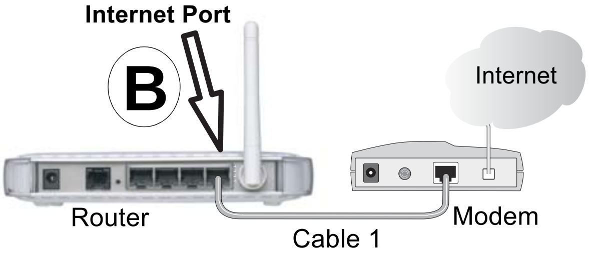


Figure 3-2: Connect the wireless router to the modem

Note: Place the WGR613VAL wireless router in a location which conforms to the "Observe Performance, Placement, and Range Guidelines" on page 4-1. The stand provided with the wireless router provides a convenient, space-saving way of installing the wireless router. Avoid stacking it on other electronic equipment.

f. Securely insert the cable that came with your wireless router (the NETGEAR cable in the diagram below) 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).

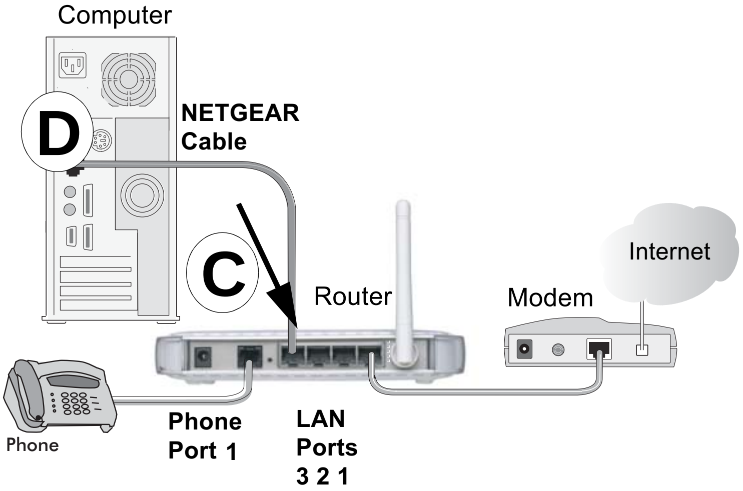


Figure 3-3: Connect the computer to the wireless router

If you have a voice service or plan to order it, connect a telephone to Phone Port 1 on the wireless router using a standard phone cord (not included).

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, plug in and turn on the broadband modem. Wait about 2 minutes.

b. Now, plug in the power cord to your wireless router. Wait about 2 minutes.

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.”

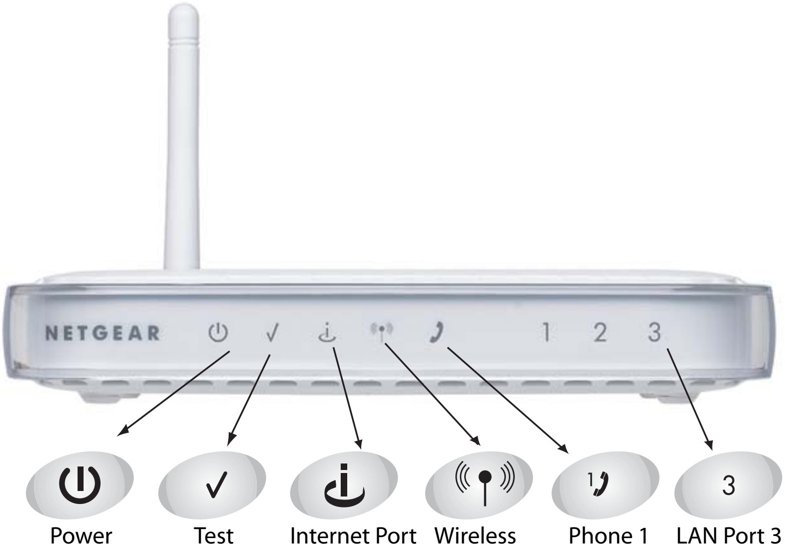


Figure 3-4: Verify the connections according to the status lights on the wireless router

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

- *Power*: The power light should turn solid green. If it does not, see "Troubleshooting Tips" on page 3-9.
- *Test*: The test light should be off. The test light blinks when the router is first turned on then goes off. If after 2 minutes it is still on, see the Troubleshooting Tips below.
- *Internet*: The Internet port light should be lit. If not, make sure the Ethernet cable is securely attached to the wireless router Internet port and the modem, and the modem is powered on.
- *Wireless:* The wireless lights should be lit. If not, see "Troubleshooting Tips" on page 3-9.
- *LAN*: A LAN light should be lit. Green indicates your computer is communicating at 100 Mbps; yellow indicates 10 Mbps. If a LAN light is not lit, check that the Ethernet cable from the computer to the router is securely attached at both ends, and that the computer is turned on.
- *Phone*: The Phone light will not be lit until your phone service provider provisions the phone service. Check the user guide from your phone service provider for details on provisioning the phone service.

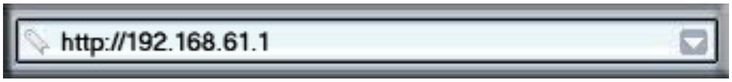
3. OPEN A BROWSER AND LOG IN TO THE ROUTER

For DSL customers, if your Internet service provider had you install software logs you in to the Internet, *do not* run that software. If such software automatically starts when you open a browser, you may need to go to the Internet Explorer Tools menu, Internet Options, Connections tab page where you can select “Never dial a connection.”

1. From the Ethernet connected computer you just set up, open a browser such as Internet Explorer or Netscape® Navigator.

   Note: If your browser connects you to the Internet, you can skip this section and proceed to the Now, Set Up a Computer for Wireless Connectivity section below.

2. Connect to the wireless router by typing **http://192.168.61.1** in the address field of your browser, then click **Enter**.

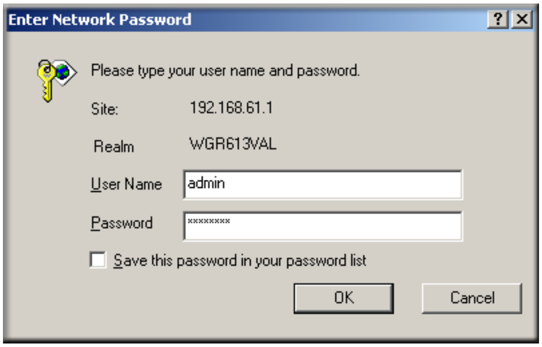


http://192.168.61.1

3. 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.

   A login window like the one shown below opens:



Enter Network Password

Please type your user name and password.

Site: 192.168.61.1

Realm WGR613VAL

User Name admin

Password ********

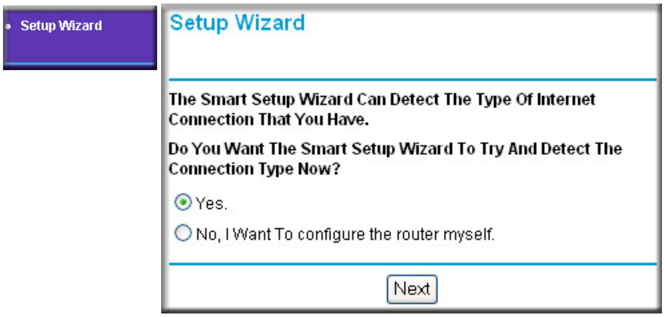
□ Save this password in your password list

Figure 3-5: Login window

Note: If you cannot connect to the wireless router, verify your cables are connected correctly, that the router is powered on, and that the networking setup of your computer is set to obtain its settings automatically via DHCP. It should be set to obtain *both* IP and DNS server addresses automatically, which is usually so. For help with this, please see the tutorials on the CD.

After logging in to the router, you will see the Internet connection Smart Wizard on the settings main page.

Use the Smart Wizard to Configure Your Wireless Router



Setup Wizard

The Smart Setup Wizard Can Detect The Type Of Internet Connection That You Have.

Do You Want The Smart Setup Wizard To Try And Detect The Connection Type Now?

● Yes.

○ No, I Want To configure the router myself.

1. You are now connected to the router. If you do not see the menu above, click the Setup Wizard link on the upper left of the main menu.
2. Click **Next** to proceed. Input your ISP settings, as needed.

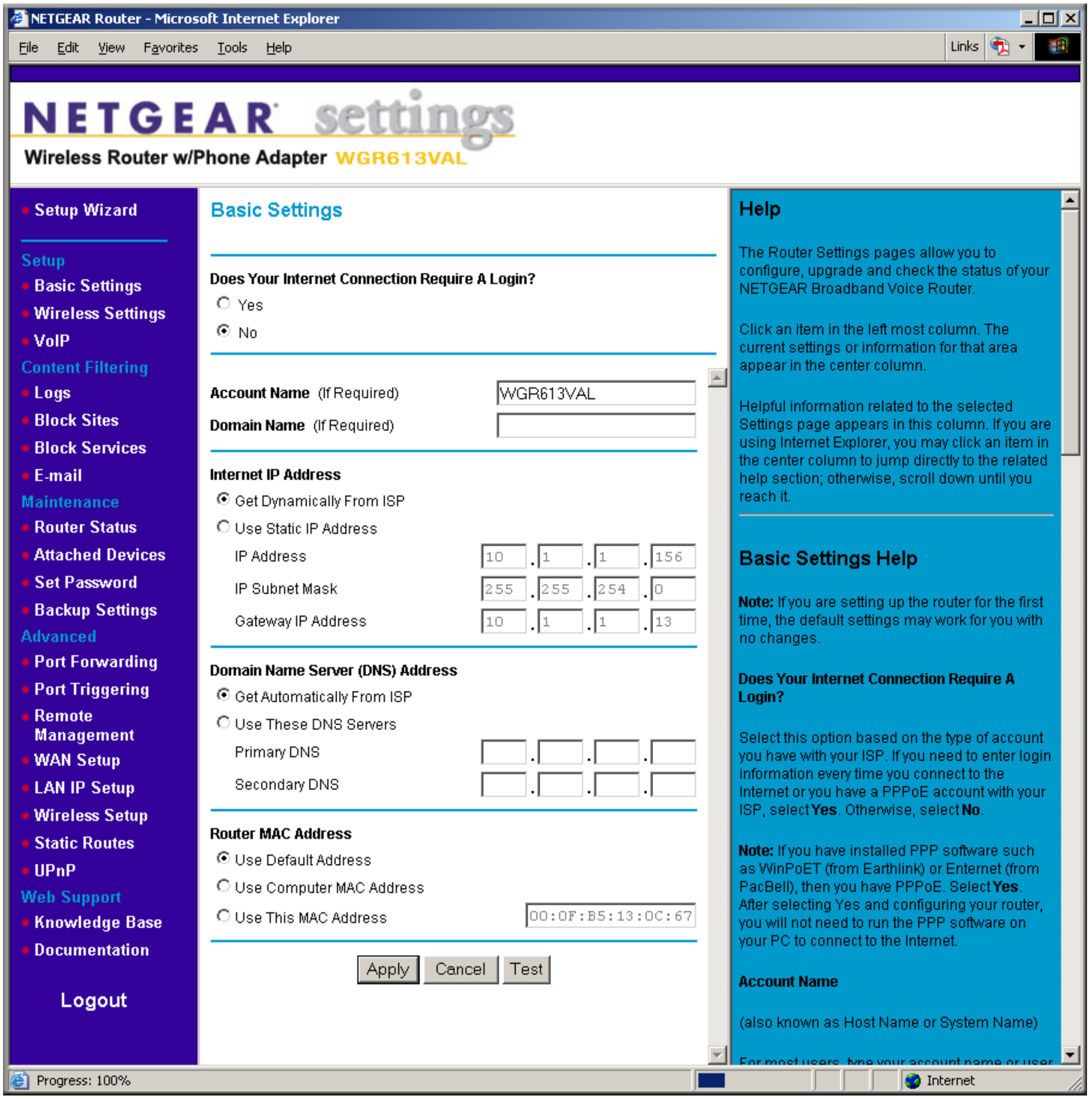
   Note: If you choose not to use the Setup Smart Wizard, you can manually configure your Internet connection settings by following the procedures in the Setup Manual on the CD.

   Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP.
3. 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 modem.
4. The Setup Smart Wizard will report the type of connection it finds and prompts you for the settings.

5. At the end of the Setup Wizard, click the **Test** button to verify your Internet connection and register your product.

   If you have trouble connecting to the Internet, use the Basic Setup Troubleshooting Tips below to correct basic problems, or refer to the Setup Manual on the CD.

   Below is the login result page.



NETGEAR Router - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
NETGEAR settings
Wireless Router w/Phone Adapter WGR613VAL

Basic Settings

Does Your Internet Connection Require A Login?

○ Yes
● No

Account Name (If Required) WGR613VAL

Domain Name (If Required)

Internet IP Address

● Get Dynamically From ISP
○ Use Static IP Address

IP Address	10 . 1 . 1 . 156
IP Subnet Mask	255 . 255 . 254 . 0
Gateway IP Address	10 . 1 . 1 . 13

Domain Name Server (DNS) Address

● Get Automatically From ISP
○ Use These DNS Servers

Primary DNS
Secondary DNS

Router MAC Address

● Use Default Address
○ Use Computer MAC Address
○ Use This MAC Address 00:0F:B5:13:0C:67

Help

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

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

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

Basic Settings Help

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

Does Your Internet Connection Require A Login?

Select this option based on the type of account you have with your ISP. If you need to enter login information every time you connect to the Internet or you have a PPPoE account with your ISP, select **Yes**. Otherwise, select **No**.

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

Account Name

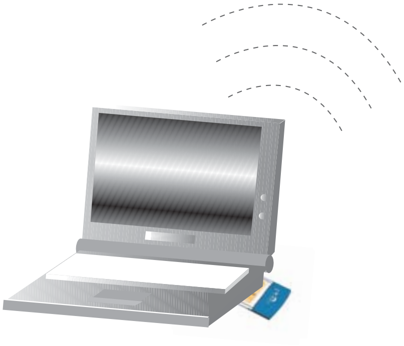
(also known as Host Name or System Name)

For most users, type your account name or user

Figure 3-6: Login Result page

You are now connected to the Internet and the wireless feature of the wireless router is enabled! Next, configure your wireless computer.

Now, Set Up a Computer for Wireless Connectivity



Wireless Adapter in a Notebook Computer

Configure the wireless adapter to match your wireless router settings exactly. If you changed the default Network Name (SSID), be sure to use what you set in the wireless router.

WIRELESS FEATURE	DEFAULT SETTING
802.11g Network Name (SSID)	**NETGEAR**
WEP or WPA Security	**Disabled**

Warning: The Network Name (SSID) is case sensitive. Typing nETgear for the SSID will not work.

Note: If your wireless adapter does not support WPA, you must reconfigure the wireless router according to the options available on your wireless adapter.

If you need to verify the wireless settings of your wireless router, go to a computer that is connected via an Ethernet cable to the wireless router and simply open a browser. Enter **http://192.168.61.1** in your browser. Then, when prompted, enter **admin** as the user name and **password** for the password both in lower case letters.

You are now wirelessly connected to the Internet with strong security!

Troubleshooting Tips

Here are some tips for correcting simple problems you may have.

Be sure to restart your network in this sequence:

1. Turn off *and* unplug the modem, turn off the wireless router, and turn off the computer
2. Turn on the modem, wait two minutes
3. Turn on the wireless router and wait 1 minute
4. Turn on the computer.

Make sure the Ethernet cables are securely plugged in.

- The Internet status light on the wireless router will be lit if the Ethernet cable to the wireless router from the modem is plugged in securely and the modem and wireless router are turned on.
- For each powered on computer connected to the wireless router with a securely plugged in Ethernet cable, the corresponding wireless router LAN port status light will be lit. The label on the bottom of the wireless router identifies the number of each LAN port.

Make sure the wireless settings in the computer and router match exactly.

The Wireless Network Name (SSID) and security settings of the router and wireless computer must match exactly.

Make sure the network settings of the computer are correct.

- LAN and wirelessly connected computers *must* be configured to obtain an IP address automatically via DHCP. Please see Appendix C, “Preparing Your Network” or the animated tutorials on the CD for help with this.
- Some cable modem ISPs require you to use the MAC address of the computer registered on the account. If so, in the Router MAC Address section of the Basic Settings menu, select “Use this Computer’s MAC Address.” The router will then capture and use the MAC address of the computer that you are now using. You must be using the computer that is registered with the ISP. Click **Apply** to save your settings. Restart the network in the correct sequence.

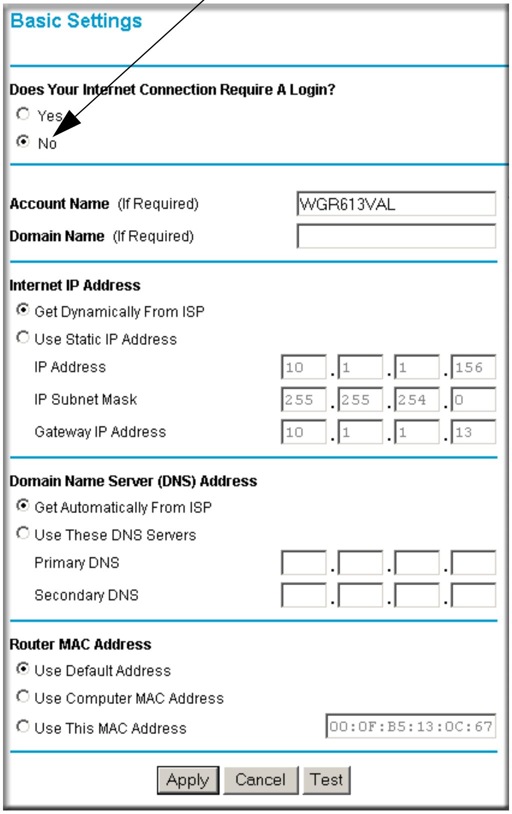
Check the router status lights to verify correct router operation.

- If the Power light does not turn solid green within 2 minutes after turning the router on, reset the router according to the instructions in “Restoring the Default Configuration and Password” on page 8-7.
- If the Wireless light does not come on, verify that the wireless feature is turned on according to the instructions in “Understanding Wireless Settings” on page 4-3.

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.

ISP *Does Not* Require Login



Basic Settings

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

Account Name (If Required): WGR613VAL
Domain Name (If Required):

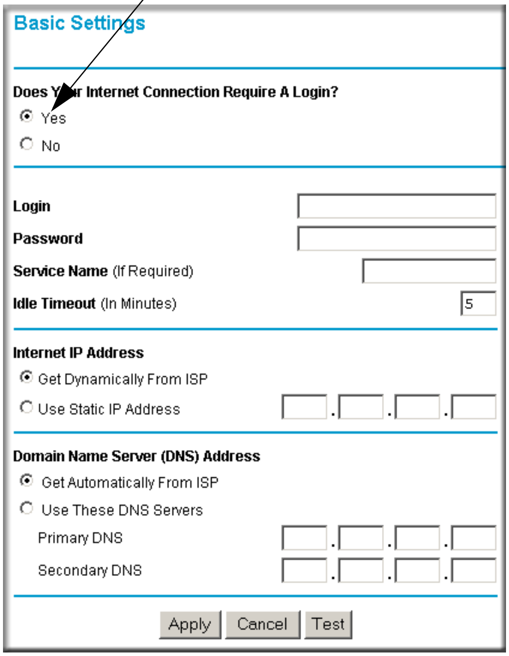
Internet IP Address
● Get Dynamically From ISP
○ Use Static IP Address
IP Address: 10 . 1 . 1 . 156
IP Subnet Mask: 255 . 255 . 254 . 0
Gateway IP Address: 10 . 1 . 1 . 13

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

Router MAC Address
● Use Default Address
○ Use Computer MAC Address
○ Use This MAC Address: 00:0F:B5:13:0C:67

Apply | Cancel | Test

ISP *Does* Require Login



Basic Settings

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

Login:
Password:
Service Name (If Required):
Idle Timeout (In Minutes): 5

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

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

Apply | Cancel | Test

Figure 3-7: Browser-based configuration Basic Settings menus

You can manually configure the router using the Basic Settings menu shown in Figure 3-7 using these steps:

1. Connect to the wireless router by typing **http://192.168.61.1** in the address field of your browser, then click **Enter**.

2. For security reasons, the wireless 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.
3. Click **Basic Settings** on the Setup menu.
4. 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 5.
   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 computer, select "Use static IP address". Enter the IP address that your ISP assigned. Also enter the netmask 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. Router's MAC Address:
   This 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 computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by "cloning" its MAC address.

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

   e. Click **Apply** to save your settings.
5. 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 computer in order to access the Internet. When you start an Internet application, your router will automatically log you in.

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

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

Chapter 4
Optimizing Wireless Connectivity and Security

This chapter describes how to configure the wireless features of your WGR613VAL 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.

The full manual with detailed how to instructions is available via the Documentation link in the configuration utility of the WGR613VAL wireless router.

Observe 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 computers will operate.
- In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
- Away from sources of interference, such as computers, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- Put the antenna in a vertical position for best side-to-side coverage. Put the antenna in a horizontal position for best up-and-down coverage.

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP or WPA connections can take slightly longer to establish.

Implement 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 WGR613VAL wireless router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

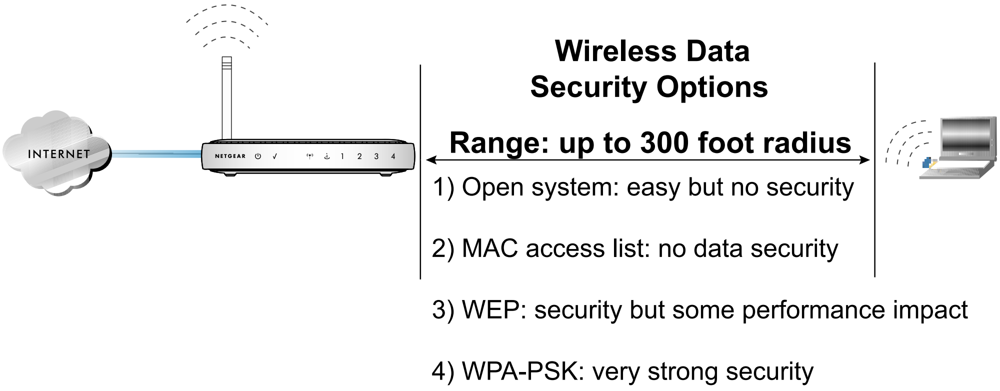

INTERNET
NETGEAR
Wireless Data Security Options
Range: up to 300 foot radius
1) Open system: easy but no security
2) MAC access list: no data security
3) WEP: security but some performance impact
4) WPA-PSK: very strong security

Figure 4-1: WGR613VAL wireless data security options

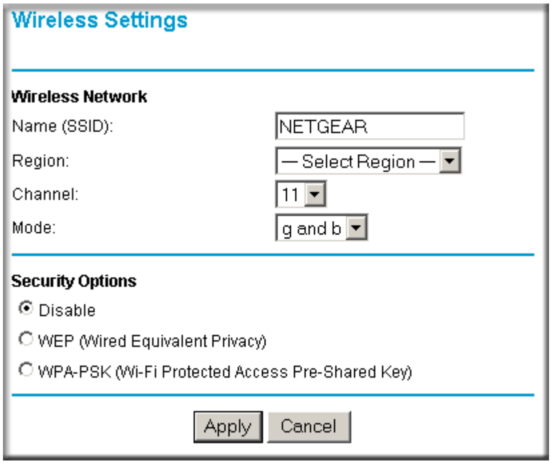
There are several ways you can enhance the security of your wireless network.

- **Restrict Access Based on MAC Address.** You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WGR613VAL. 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 LAN when you are away and the others in the household all use wired connections.

Understanding Wireless Settings

To configure the Wireless settings of your router, click the Wireless link in the main menu of the browser interface.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: — Select Region —

Channel: 11

Mode: g and b

Security Options

● Disable

○ WEP (Wired Equivalent Privacy)

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

Figure 4-2: Wireless Settings page

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

- **Placement of the Router to Optimize Wireless Connectivity**: The operating distance or range of your wireless connection can vary significantly based on the physical placement of the router. For best results, place your router:
  - Near the center of the area in which your PCs will operate
  - In an elevated location such as a high shelf
  - Away from potential sources of interference (such as PCs, microwaves, and cordless phones)

  - With the Antenna tight and in the upright position
  - Away from large metal surfaces

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

- **Wireless Network**
  - **Name (SSID)**: Enter a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is NETGEAR, but NETGEAR strongly recommends that you change your networks Name (SSID) to a different value. This value is also case-sensitive. For example, NETGEAR is not the same as NETGEAr.
  - **Region**: Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here. If your country or region is not listed, please check with your local government agency or check our website for more information on which channels to use.
  - **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.
  - **Mode**: Select the desired wireless mode. The options are:
    - **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.

    The default is "g & b", which allows both "g" and "b" wireless stations to access this device.
- **Security Options**
  - **Disable: no data encryption**
  - **WEP (Wired Equivalent Privacy)**: use WEP 64 or 128 bit data encryption
  - **WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)**: use WPA-PSK standard encryption

- **Security Encryption (WEP)**
  - **Authentication Type**: Normally this can be left at the default value of "Automatic." If that fails, select the appropriate value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.
    - **Open System**: With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the WGR613VAL *does* perform 64- or 128-bit data encryption but *does not* perform any authentication.
    - **Shared Key**: Shared Key authentication encrypts the SSID and data.
  - **Encryption Strength**: Select the WEP Encryption level:
    - 64-bit (sometimes called 40-bit) encryption
    - 128-bit encryption
- **Security Encryption (WEP) Key**: If using WEP, 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 Key Generation (Passphrase)**: Enter a word or group of printable characters in the Passphrase box and click the Generate button to automatically configure the WEP Key(s). If encryption strength is set to 64 bit, then each of the four key boxes will automatically be populated with key values. If encryption strength is set to 128 bit, then only the selected WEP key box will automatically be populated with key values.
  - **Manual Entry Mode**: Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key box.
    - For 64 bit WEP: Enter ten hexadecimal digits (any combination of 0-9, A-F).
    - For 128 bit WEP: Enter twenty-six hexadecimal digits (any combination of 0-9, A-F).
- **Security Encryption (WPA-PSK)**: Enter a word or group of printable characters in the Passphrase box. The Passphrase must be 8 to 63 characters in length (these characters are case sensitive). WPA-Pre-shared Key *does* perform authentication, uses 128-bit data encryption and dynamically changes the encryption keys making it nearly impossible to circumvent.

  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.

  Key Lifetime: This setting determines how often the encryption key is changed. Shorter periods provide greater security, but adversely affect performance. If desired, you can change the default value.

Information to Gather Before Changing Basic Wireless Settings

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

- **802.11g Wireless Network Name (SSID)*:*** ______________________________

  The SSID, identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID *is* case sensitive. The SSID in the wireless adapter card must match the SSID of the wireless router. In some configuration utilities (such as in Windows XP), the term “wireless network name” is used instead of SSID.

- **If WEP Authentication is Used.** Circle one: **Open System**, **Shared Key, or Auto**.

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

  – **WEP Encryption key size**. Choose one: **64-bit** or **128-bit**. Again, the encryption key size must be the same for the wireless adapters and the wireless router.

  – **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.

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

    Key 1: ___________________________________

    Key 2: ___________________________________

    Key 3: ___________________________________

    Key 4: ___________________________________

- **If WPA-PSK Authentication is Used.**

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

Use the procedures described in the reference manual to configure the WGR613VAL.

Default Factory Settings

When you first receive your WGR613VAL, the default factory settings are shown below. You can restore these defaults with the Factory Default Restore button on the rear panel. After you install the WGR613VAL wireless router, use the procedures below to customize any of the settings to better meet your networking needs.

WIRELESS FEATURE	DEFAULT SETTING
Wireless Access Point	**Enabled**
Wireless Access List (MAC Filtering)	**All wireless stations allowed**
SSID broadcast	**Enabled**
Network Name (SSID)	**NETGEAR**
WPA and WEP Security	**Disabled**

Warning: The Network Name (SSID) and passphrase are case sensitive. Typing nETgear for the SSID will not work.

Chapter 5
Content Filtering

This chapter describes how to use the content filtering features of the WGR613VAL Wireless Router and Voice Adapter to protect your network. These features can be found by clicking on the Content Filtering heading in the Main Menu of the browser interface.

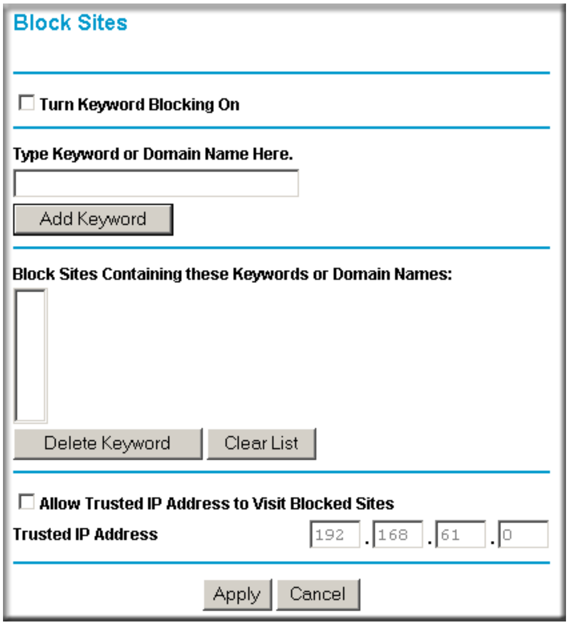
Content Filtering Overview

The WGR613VAL Wireless Router and Voice Adapter provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time of day, Web addresses and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

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

Blocking Access to Internet Sites

The WGR613VAL wireless router allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is shown in Figure 5-1 below:


Block Sites

□ Turn Keyword Blocking On

Type Keyword or Domain Name Here.

Block Sites Containing these Keywords or Domain Names:

□ Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address: 192 . 168 . 61 . 0

Figure 5-1: Block Sites menu

If you want to limit access to certain sites on the Internet, you need to set up content filtering.

There are two ways to filter content:

- blocking access to certain domains (for example, www.badstuff.com/XXX)
- blocking sites that contains certain words (like profanity or explicit sexual material).

  Keyword application examples:

  – If the keyword “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.

  – If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.

  - If you wish to block all Internet browsing access during a scheduled period, enter the keyword “.” and set the schedule in the Schedule menu.

When users try to access a blocked site, they will get a message: "Blocked by NETGEAR".

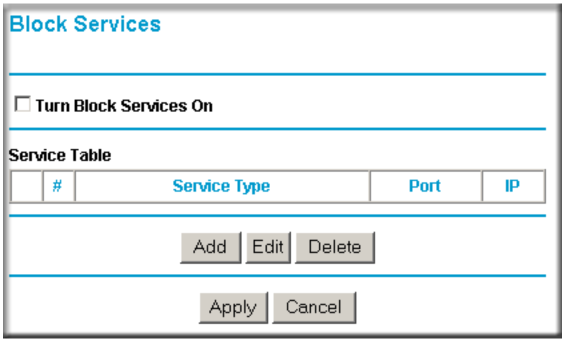
- To enable blocking by Keywords or Internet Domains, check the Turn Keyword Blocking On checkbox.
- To Disable the Block Sites feature, uncheck the Turn Keyword Blocking On checkbox.
- To Add Keywords Or Internet Domains:
  a. In the box where you see Type Keyword Or Domain Name Here, type the word or domain name you want to block.
  b. Click Add Keyword.
  c. The word or domain name will appear in the list below.
  d. Continue adding names and keywords until you are finished.
  e. Click Apply when finished.
- Block List: The list under the heading "Block Sites Containing these Keywords or Domain Names" contains the current list of items to block.
- To Delete A Keyword Or Domain Name:
  a. Select the word or domain name in the list.
  b. Click Delete Keyword.
  c. Continue selecting and deleting names and keywords until you are finished.
  d. Click Apply.
- To Delete All Keywords And Domain Names:
  a. Click Clear List.
  b. Click Apply.
- To Allow One Computer To Have Unrestricted Access To The Internet:
  a. Select the Allow Trusted IP Address To Visit Blocked Sites check box.
  b. Type the IP address of the computer in the Trusted IP Address area.

     You should only need to type a number in the last box. 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.

- To Allow Unrestricted Access To The Internet:
  a. Select Never in the Keyword Blocking menu.
  b. Click Apply.

Blocking Access to Internet Services

The WGR613VAL wireless router allows you to block the use of certain Internet services by PCs on your network. This is called services blocking or port filtering. The Block Services menu is shown below:


Block Services

☐ Turn Block Services On

Service Table

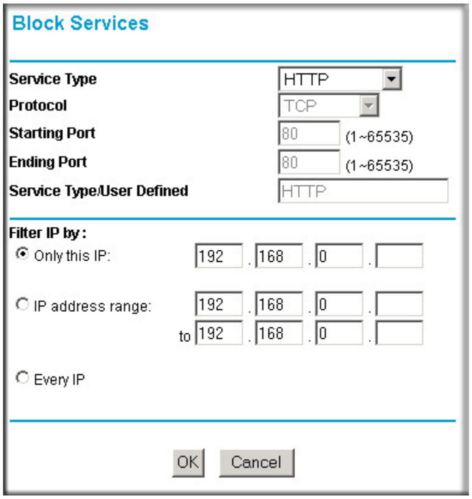
	#	Service Type	Port	IP

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 Add Services menu will appear, as shown below:



Block Services

Service Type	HTTP
Protocol	TCP
Starting Port	80 (1~65535)
Ending Port	80 (1~65535)
Service Type/User Defined	HTTP

Filter IP by :

● Only this IP: 192 . 168 . 0 .

○ IP address range: 192 . 168 . 0 . to 192 . 168 . 0 .

○ Every IP

Figure 5-3: Add Services 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.

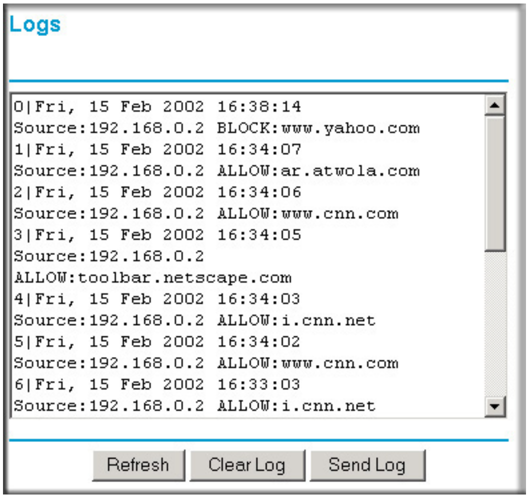
If you know that the application uses either TCP or UDP, select the appropriate protocol. If you are not sure, select Both.

Configuring Services Blocking by IP Address Range

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

Viewing Logs of Web Access or Attempted Web Access

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



Logs

```
0|Fri, 15 Feb 2002 16:38:14
Source:192.168.0.2 BLOCK:www.yahoo.com
1|Fri, 15 Feb 2002 16:34:07
Source:192.168.0.2 ALLOW:ar.atwola.com
2|Fri, 15 Feb 2002 16:34:06
Source:192.168.0.2 ALLOW:www.cnn.com
3|Fri, 15 Feb 2002 16:34:05
Source:192.168.0.2
ALLOW:toolbar.netscape.com
4|Fri, 15 Feb 2002 16:34:03
Source:192.168.0.2 ALLOW:i.cnn.net
5|Fri, 15 Feb 2002 16:34:02
Source:192.168.0.2 ALLOW:www.cnn.com
6|Fri, 15 Feb 2002 16:33:03
Source:192.168.0.2 ALLOW:i.cnn.net
```

Figure 5-4: 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. 128 entries are available numbered from 0 to 127. The log will keep the record of the latest 128 entries.
Date and Time	The date and time the log entry was recorded.

Table 5-1. Log entry descriptions

Field	**Description**
Source IP	The IP address of the initiating device for this log entry.
Action	This field displays whether the access was blocked or allowed.
	The name or IP address of the Web site or newsgroup visited or attempted to access.

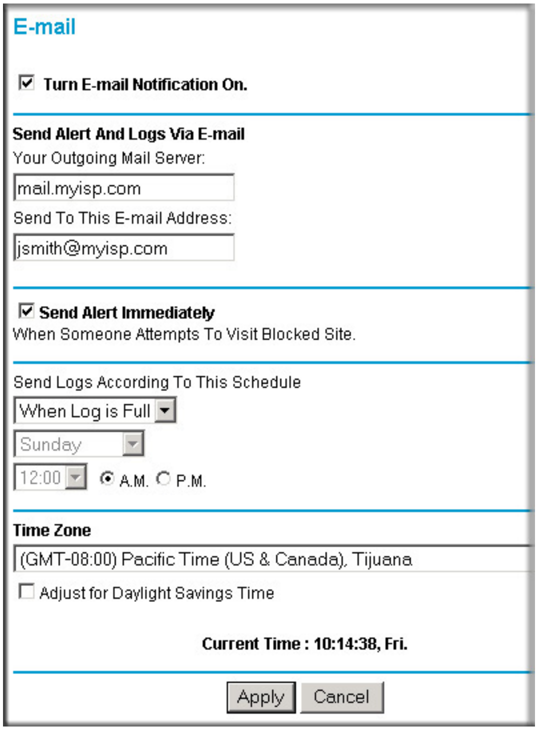
Log action buttons are described in Table 5-2

Table 5-2. Log action buttons

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

Configuring E-Mail Alert and Web Access Log Notifications

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



E-mail

☑ Turn E-mail Notification On.

Send Alert And Logs Via E-mail

Your Outgoing Mail Server: mail.myisp.com

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

☑ Send Alert Immediately

When Someone Attempts To Visit Blocked Site.

Send Logs According To This Schedule

When Log is Full

Sunday

12:00 ● A.M. ○ P.M.

Time Zone

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

□ Adjust for Daylight Savings Time

Current Time : 10:14:38, Fri.

Figure 5-5: Email menu

- Turn e-mail notification on
  Check this box if you wish to receive e-mail logs and alerts from the router.
- Your outgoing mail server
  Enter the name of your ISP’s outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.

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

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

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

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

The WGR613VAL wireless router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

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

Chapter 6
Doing Basic Router Housekeeping

This chapter describes how to use some of the maintenance features of your WGR613VAL Wireless Router and Voice Adapter. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface. Other maintenance features not presented in this chapter can be found accessed via links in the browser interface of the wireless router to the documentation and in the help screens.

Changing the Administrator Password

The default password for the wireless router's Web Configuration Manager is **password**. 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.

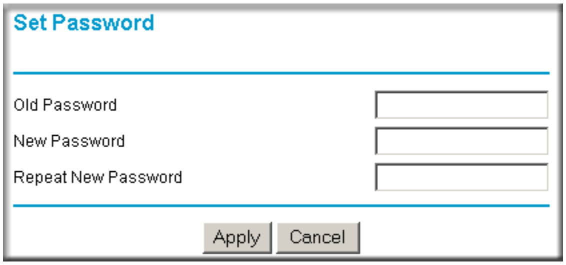
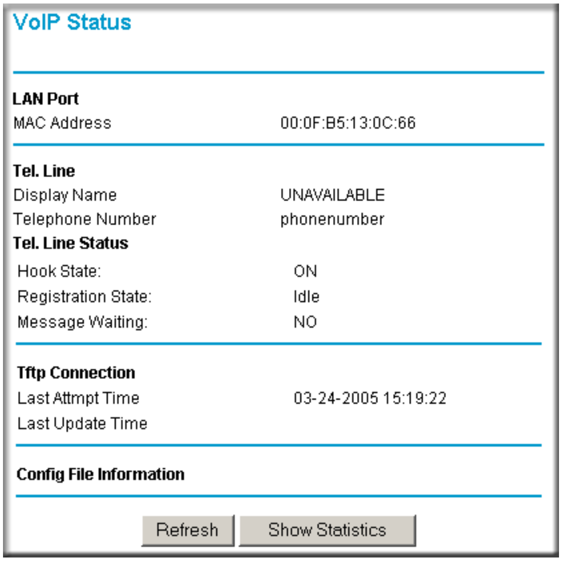


Figure 6-1: Set Password menu

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

VoIP Status

From the Main Menu of the browser interface, under the Setup heading, select the VoIP link display the menu shown below.



VoIP Status

LAN Port

MAC Address 00:0F:B5:13:0C:66

Tel. Line

Display Name UNAVAILABLE

Telephone Number phonenumber

Tel. Line Status

Hook State: ON

Registration State: Idle

Message Waiting: NO

Tftp Connection

Last Attmpt Time 03-24-2005 15:19:22

Last Update Time

Config File Information

Figure 6-2: VoIP Status

This page shows the current status of your VoIP (Voice over Internet Protocol) connection.

- **LAN Port**

  MAC Address: the physical address of the WGR613VAL, as seen from the local LAN.

- **Tel. Line**
  - **Display Name**: This is the name you have already chosen when you first opened your account. Your "Display Name" will be visible to other individuals with caller ID.

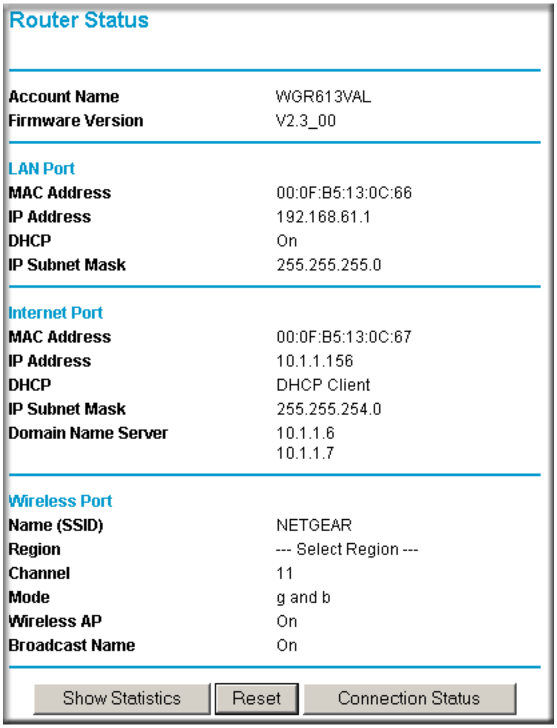
    If your display name appears as "UNAVAILABLE", either your account with your VoIP service provider has not been established or your router has been unable to connect to the Internet.
  - **Telephone Number:** This is the telephone number other people will use when they call you. This number was assigned to your router when you first established your account. Each line can have a different telephone number.

If your Telephone Number appears as "phonenumber", either your account with your VoIP service provider has not been established or your router has been unable to connect to the Internet.

- **Line Status**
  - **Hook State**: The "Hook State" displays the condition of the telephone receiver. ON indicates the receiver is "on-the-hook", while OFF indicates the receiver is "off-the-hook".
  - **Registration State**: When your router has successfully connected to the VoIP servers, the "Registration State" will be displayed as "Success". However, if you do not have a VOIP account or if the router could not connect to the VoIP servers, the "Registration State" will be displayed as "Idle".
  - **Message Waiting**: The "Message Waiting" status indicates if you have a new message waiting in your voice mail box.

Router Status

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Status link display the menu shown below.



Router Status

Account Name	WGR613VAL
Firmware Version	V2.3_00
LAN Port	
MAC Address	00:0F:B5:13:0C:66
IP Address	192.168.61.1
DHCP	On
IP Subnet Mask	255.255.255.0
Internet Port	
MAC Address	00:0F:B5:13:0C:67
IP Address	10.1.1.156
DHCP	DHCP Client
IP Subnet Mask	255.255.254.0
Domain Name Server	10.1.1.6 10.1.1.7
Wireless Port	
Name (SSID)	NETGEAR
Region	--- Select Region ---
Channel	11
Mode	g and b
Wireless AP	On
Broadcast Name	On

Figure 6-3: Router Status page

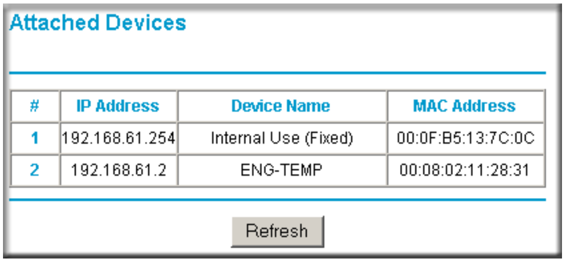
You can use the Router Status page to check the current settings and statistics for your router. This page shows you the current settings. If something needs to be changed, you'll have to change it on the relevant page.

- **Account Name**: This is the Account Name that you entered in the Setup Wizard or Basic Settings.
- **Firmware Version**: This is the current software the router is using. This will change if you upgrade your router.

- **LAN Port**: These are the current settings, as set in the LAN IP Setup page.
  - **MAC Address**: the physical address of the WGR613VAL, as seen from the local LAN.
  - **IP Address**: LAN IP address of the Router.
  - **DHCP**: indicates if the WGR613VAL is acting as a DHCP Server for devices on your LAN.
  - **IP Subnet Mask**: subnet mask associated with the LAN IP address.
- **Wireless Port**: These are the current settings, as set in the Wireless Settings page.
  - **Name (SSID)**: SSID of the WGR613VAL.
  - **Region**: the location (country).
  - **Channel**: the current channel in use.
  - **Mode**: indicates the current mode (g & b, g, or b)
  - **Wireless AP**: indicates if the Access Point feature of the WGR613VAL is enabled or not. If not enabled, the Wireless LED on the front panel will be off.
  - **Broadcast Name**: indicates if the WGR613VAL is broadcasting its SSID.
- **Internet Port**: These are the current settings that you set in the Setup Wizard or Basic Settings pages.
  - **MAC Address**: the physical address of the WGR613VAL, as seen from the Internet.
  - **IP Address**: current Internet IP address. If assigned dynamically, and no Internet connection exists, this will be blank or 0.0.0.0
  - **DHCP**: indicates either Client (IP address is obtained dynamically) or None.
  - **IP Subnet Mask**: the subnet mask associated with the Internet IP address Domain Name Server - displays the address of the current DNS.
- Click the Connection Status button to see information about your current Internet connection.
- Click Reset to reset (restart) the router.
- Click Show Statistics to see router performance statistics such as the number of packets sent and number of packets received for each port.

Attached Devices

From the Main Menu of the browser interface, under the Maintenance heading, select the Attached Devices link display the menu shown below.



Attached Devices

#	IP Address	Device Name	MAC Address
1	192.168.61.254	Internal Use (Fixed)	00:0F:B5:13:7C:0C
2	192.168.61.2	ENG-TEMP	00:08:02:11:28:31

Figure 6-4: Attached Devices page

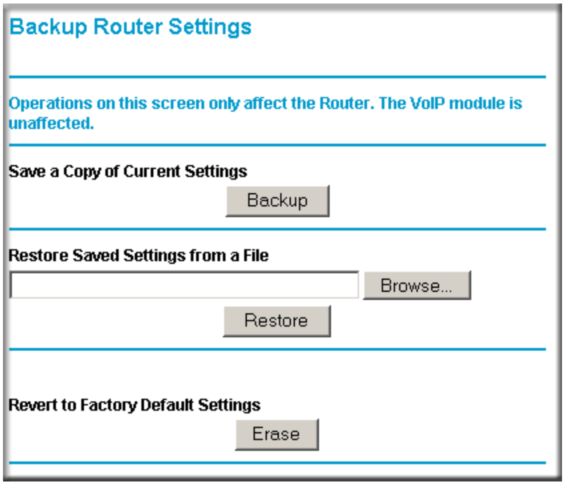
This page shows the IP Address, Device Name and MAC (Media Access Control) Address for each computer attached to the router.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click on the Refresh button.

➡	**Note:** The LAN IP address of 192.168.61.254 is used internally by the voice adapter.

Backup Settings

From the Main Menu of the browser interface, under the Maintenance heading, select the Backup Settings link display the menu shown below.


Backup Router Settings

Operations on this screen only affect the Router. The VoIP module is unaffected.

Save a Copy of Current Settings

Restore Saved Settings from a File

Revert to Factory Default Settings

Figure 6-5: Backup Router Settings page

This page allows you to backup, restore and erase the router's current settings.

Note: Operations on this screen only affect the Router. The VoIP module is unaffected.

Once you have the router working properly, you should backup the information to have it available if something goes wrong. When you backup the settings, they are saved as a file on your computer. You can restore the router's settings from this file.

IMPORTANT! Once you start restoring settings or erasing the router, do NOT try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting! This should only take a minute or so. When the Test light stops blinking, wait a few more seconds before doing anything with the router.

- **Save (Backup)**: To create a backup file of the current settings:
  a. Click Backup.
  b. If you don't have your browser set up to save downloaded files automatically, locate where you want to save the file, rename it if you like, and click Save.

If you have your browser set up to save downloaded files automatically, the file is saved to the your browser's download location on the hard disk and is called netgear.cfg.

- **Restore**: To restore settings from a backup file:

  a. Click Browse.

  b. Locate and select the previously saved backup file (by default, netgear.cfg).

  c. Click Restore.

  A window appears letting you know that the router has been successfully restored to previous settings. The router will restart. This will take about one minute.

  IMPORTANT! Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until it finishes restarting! When the Test light stops blinking, wait a few more seconds before doing anything with the router.

  d. Close the message window.

- **Revert (Erase)**: To erase the current settings and reset the router to the original factory default settings:

  a. Click Erase.

  IMPORTANT! Do not try to go online, turn off the router, shutdown the computer or do anything else to the router until the router finishes restarting! When the Test light stops blinking, wait a few more seconds before doing anything with the router.

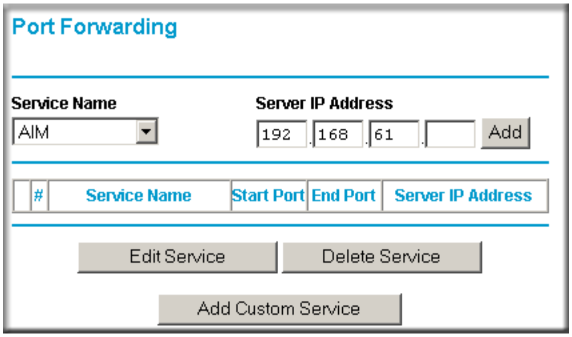
  After you have erased the router's current settings, the router's password will be password, the LAN IP address will be 192.168.61.1 and the router will act as a DHCP server on the LAN and act as a DHCP client to the Internet.

Chapter 7
Setting Up Advanced Router Configurations

This chapter describes how to configure some of the advanced setup features of your WGR613VAL Wireless Router and Voice Adapter. These features can be found by clicking on the Advanced heading in the Main Menu of the browser interface. Features not presented in this chapter are presented in the User Guide and help screens available by following the links in the browser interface of the wireless router.

Port Forwarding

Using the Port Forwarding 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). For the services, applications, or games, that already exist in the pull-down list, you'll 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 Forwarding

Service Name: AIM

Server IP Address: 192 . 168 . 61 .

	#	Service Name	Start Port	End Port	Server IP Address

Figure 7-1: Port Forwarding page

- **Port Assignment**: You may make up to 20 different port assignments for Internet services, applications or games. In the Service Name lists, you'll be able to select either a service, application or game. If you don't 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'll need to determine which type of services you'll 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 setup a computer or server to be accessible to the Internet for an Internet service:

  a. Select the Internet service you want to use from the Service Name list.

  b. Type the IP address of the computer in the Server IP Address box.

  c. Click 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**: Before starting, you'll need to know which service, application or game you'll be configuring. Also, you'll need to have the IP address for the computer that you want to use.

  To setup a computer to play Internet games or use Internet applications:

  a. Select the Internet application or game you want to use from one of the relevant lists.

     The Start Port and End Port boxes are filled in.

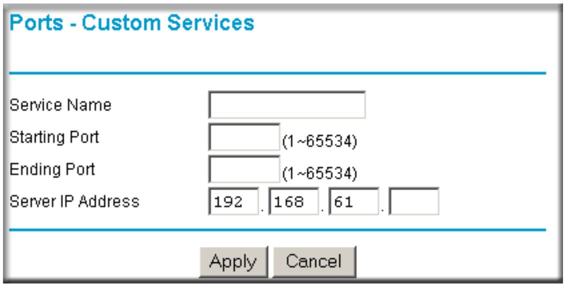
     Note: If you can't find the game or application you want in one of the lists, click Add Custom Service button, and type the Service Name, Starting Port, Ending Port, and Server IP Address information.

  b. Type the IP address of the computer in the Server IP Address box.

  c. Click Add button.

- **To setup an additional computer to play, for example, Hexen II or KALI**:

  a. Click the button of Add Custom Service.



Ports - Custom Services

Service Name
Starting Port (1~65534)
Ending Port (1~65534)
Server IP Address 192 . 168 . 61 .

Figure 7-2: Custom Services page

b. Type the service name in the Service Name box.

c. 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've 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.

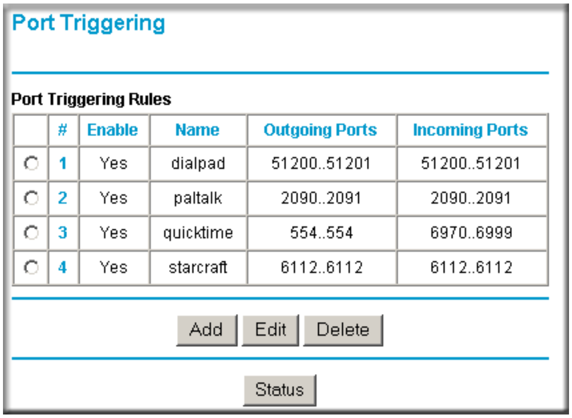
d. Type the same port number in the Ending Port box.

e. Type the IP address of the computer in the Server IP Address box.

f. Click Apply button.

Port Triggering

Port Triggering is used to allow applications which would otherwise be blocked by the router. Using this feature requires that you know the port numbers used by the Application.



Port Triggering

Port Triggering Rules

	#	Enable	Name	Outgoing Ports	Incoming Ports
○	1	Yes	dialpad	51200..51201	51200..51201
○	2	Yes	paltalk	2090..2091	2090..2091
○	3	Yes	quicktime	554..554	6970..6999
○	4	Yes	starcraft	6112..6112	6112..6112

Figure 7-3: Port Triggering page

Once configured, operation is as follows:

1. A PC makes an outgoing connection using a port number defined in the Port Triggering table.
2. This Router records this connection, opens the INCOMING port or ports associated with this entry in the Port Triggering table, and associates them with the PC.
3. The remote system receives the PCs request, and responds using a different port number.

4. This Router matches the response to the previous request, and forwards the response to the PC.

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

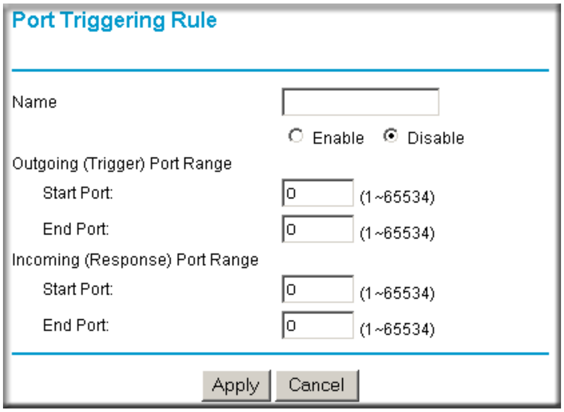
Notes:

- Only 1 PC can use a "Port Triggering" application at any time.
- After a PC has finished using a "Port Triggering" application, there is a "Time-out" period before the application can be used by another PC. This is required because this Router cannot be sure when the application has terminated.

Port Triggering Rules: This table lists the current rules:

- Enable: Indicates if the rule is enabled or disabled. Generally, there is no need to disable a rule unless it interferes with some other function, such as Port Forwarding.
- Name: The name for this rule.
- Outgoing Ports: The port or port range for outgoing traffic. An outgoing connection using one of these ports will "Trigger" this rule.
- Incoming Ports: The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule.

Adding a new Rule: To add a new rule, click Add:



Port Triggering Rule

Name

○ Enable ● Disable

Outgoing (Trigger) Port Range

Start Port: 0 (1~65534)

End Port: 0 (1~65534)

Incoming (Response) Port Range

Start Port: 0 (1~65534)

End Port: 0 (1~65534)

Figure 7-4: Port Triggering Rule Add page

Enter the following data on the resulting screen.

- Name: enter a suitable name for this rule (e.g. the name of the application)
- Enable/Disable: select the desired option.
- Outgoing (Trigger) Port Range: enter the range of port numbers used by the application when it generates an outgoing request.
- Incoming (Response) Port Range: enter the range of port numbers used by the remote system when it responds to the PC's request.

Modifying or Deleting an existing Rule:

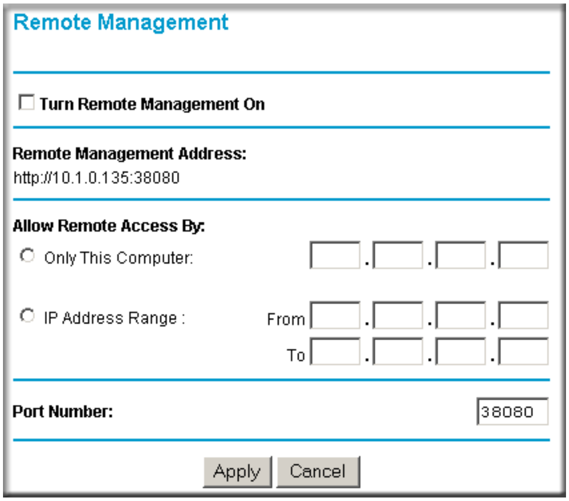
1. Select the desired rule by clicking the radio button beside the rule.
2. Click Edit or Delete as desired.

Checking Operation and Status: To see which rules are currently being used, click the Status button. The following data will be displayed:

- Rule: the name of the Rule.
- LAN IP Address: The IP address of the PC currently using this rule.
- Open Ports: the Incoming ports which are associated the this rule. Incoming traffic using one of these ports will be sent to the IP address above.
- Time Remaining: The time remaining before this rule is released, and thus available for other PCs. This timer is restarted whenever incoming or outgoing traffic is received.

Remote Management

Using the Remote Management menu, you can allow a user on the Internet to configure, upgrade and check the status of your router.



Remote Management

□ Turn Remote Management On

Remote Management Address:
http://10.1.0.135:38080

Allow Remote Access By:

○ Only This Computer: ___.___.___.___

○ IP Address Range : From ___.___.___.___ To ___.___.___.___

Port Number: 38080

Figure 7-5: Remote Management page

IMPORTANT: Be sure to change the router's default password to a very secure password.

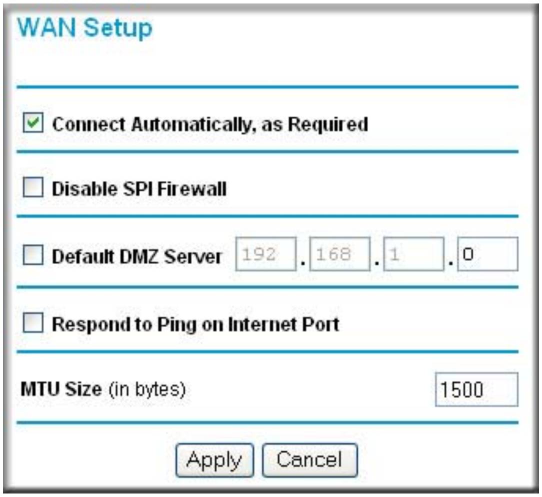
- **Turn Remote Management On**
  a. Click the check box to Turn Remote Management On.
  b. Click the Apply button to save changes.
- **Remote Management Address**: This is the current address you will use When accessing your router from the Internet. To access the router, you will type your router's 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 10.0.0.123 and you use port number 8080, enter in your browser: http://10.0.0.123:8080
- **Allow Remote Access**: For security, you should restrict access to as few external IP addresses as practical.
  – Click Only This Computer to allow access by only one IP address.

- Click IP Address Range to allow access from a range of IP addresses on the Internet, enter a beginning and ending IP address to define the allowed range.
- Click Everyone to allow access by everyone on the Internet.

- **Port Number**: 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 65534, but do not use the number of any common service port.

Configuring WAN Setup Options

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



WAN Setup

☑ Connect Automatically, as Required

□ Disable SPI Firewall

□ Default DMZ Server 192 . 168 . 1 . 0

□ Respond to Ping on Internet Port

MTU Size (in bytes) 1500

Figure 7-6: WAN Setup menu.

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 “Show WAN Status” screen.

Disable SPI Router

Normally, this option should be Enabled, so that your local network will be protected by the Stateful Packet Inspection (SPI) router included in the WGR613VAL. However, certain communications functions like VPN may require turning off the SPI feature.

Respond to Ping on Internet WAN Port

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

Setting the MTU Size

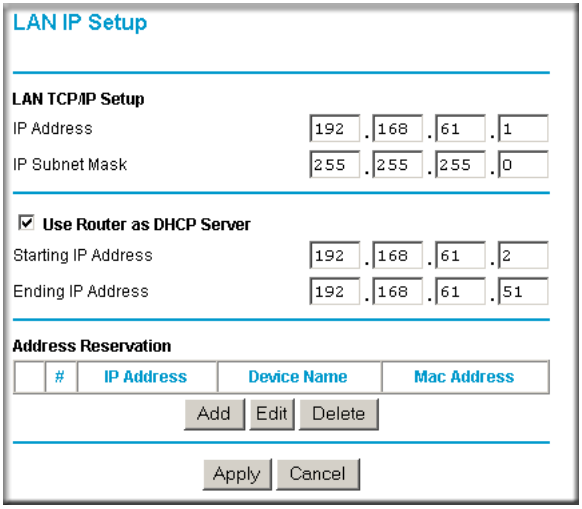
The default MTU size is usually fine. The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, particularly some using PPPoE, you may need to reduce the MTU to 1492. This should not be done unless you are sure it is necessary by your ISP.

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.

Using the LAN IP Setup Options

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



LAN IP Setup

LAN TCP/IP Setup

IP Address 192 . 168 . 61 . 1

IP Subnet Mask 255 . 255 . 255 . 0

☑ **Use Router as DHCP Server**

Starting IP Address 192 . 168 . 61 . 2

Ending IP Address 192 . 168 . 61 . 51

Address Reservation

	#	IP Address	Device Name	Mac Address

Figure 7-7: LAN IP Setup Menu

Configuring LAN TCP/IP Setup Parameters

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

- LAN IP addresses—192.168.61.1
- Subnet mask—255.255.255.0

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

The LAN IP parameters are:

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

- IP Subnet Mask
  This is the LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
- RIP Direction
  RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the router sends and receives RIP packets. 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. RIP-2B uses subnet broadcasting.

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

Using the Router as a DHCP server

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

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See "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 will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the ‘Use router as DHCP server’ check box. Otherwise, leave it checked.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.61.2 and 192.168.61.253, although you may wish to save part of the range for devices with fixed addresses.

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

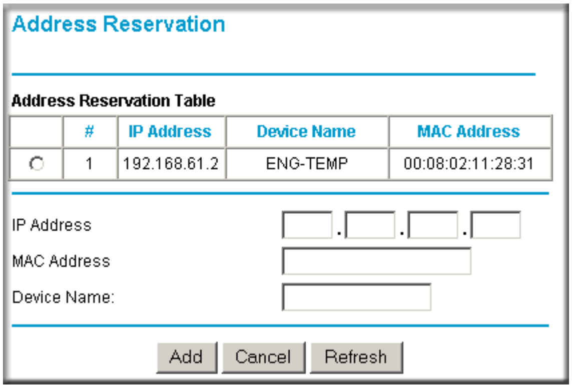
- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address (the router’s LAN IP address)
- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router’s LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address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

Using Address Reservation

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

To reserve an IP address:

1. Click the Add button.



Address Reservation

Address Reservation Table

	#	IP Address	Device Name	MAC Address
○	1	192.168.61.2	ENG-TEMP	00:08:02:11:28:31

IP Address . . .

MAC Address

Device Name:

Figure 7-8: Address Reservation page

2. In the IP Address box, type the IP address to assign to the computer or server. (choose an IP address from the router’s LAN subnet, such as 192.168.0.X)
3. Type the MAC Address of the computer or server. (Tip: If the computer is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.)
4. Click Apply to enter the reserved address into the table.

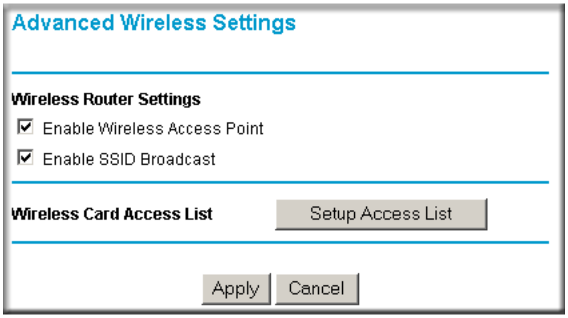
Note: The reserved address will not be assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

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

Wireless Setup

Warning: The Wireless Router is already configured with the optimum settings. Do not alter these settings unless directed by Netgear Support. Incorrect settings may disable the Wireless Router unexpectedly.



Advanced Wireless Settings

Wireless Router Settings

☑ Enable Wireless Access Point

☑ Enable SSID Broadcast

Wireless Card Access List

Figure 7-9: Advanced Wireless Settings page

- **Wireless Router Settings**
  - Enable Wireless Access Point: The Wireless Access Point of this router can be enabled or disabled to allow wireless access. The wireless icon on the front of the router will also display the current status of the Wireless Access Point to let you know if it is disabled or enabled. If Enabled, wireless stations will be able to access the LAN and Internet. If Disabled, wireless stations will not be able to access the LAN and Internet.
  - Enable SSID Broadcast: If Enabled, the Wireless Router SSID will broadcast its name (SSID) to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.
- **Wireless Card Access List**: By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses.

Click the Setup Access List button to display the Wireless Access List screen, where you can manage the list of allowed PCs.

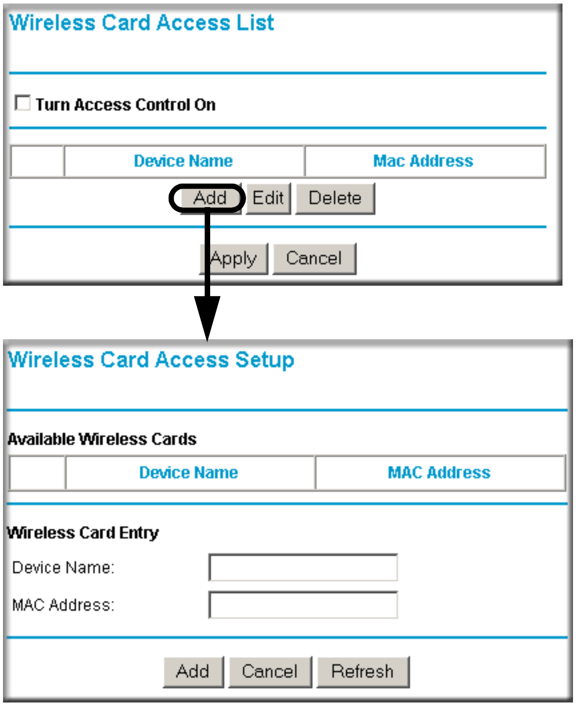
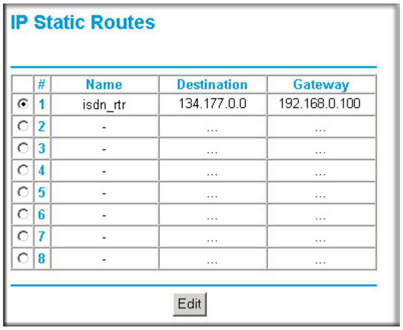


Figure 7-10: Wireless Card Access List and Setup pages

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, click on Static Routes to view the Static Route menu, shown below.



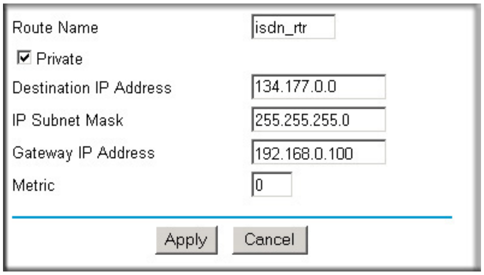
IP Static Routes

	#	Name	Destination	Gateway
●	1	isdn_rtr	134.177.0.0	192.168.0.100
○	2	-	...	...
○	3	-	...	...
○	4	-	...	...
○	5	-	...	...
○	6	-	...	...
○	7	-	...	...
○	8	-	...	...

Figure 7-11. Static Route Summary Table

To add or edit a Static Route:

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



Route Name: isdn_rtr
☑ Private
Destination IP Address: 134.177.0.0
IP Subnet Mask: 255.255.255.0
Gateway IP Address: 192.168.0.100
Metric: 0

Figure 7-12. Static Route Entry and 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.

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 192.168.0.100.
- Your company’s network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company’s router.

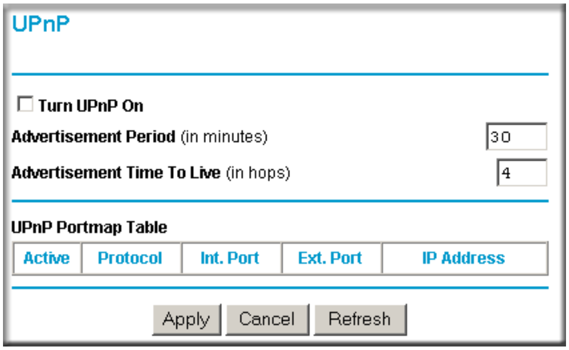
In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like Figure 7-12.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- 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.

UPnP

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



UPnP

□ Turn UPnP On

Advertisement Period (in minutes) 30

Advertisement Time To Live (in hops) 4

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address

Figure 7-13: UPnP page

- **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 advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 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. A hop is the number of steps 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 Common Problems

This chapter gives information about troubleshooting your WGR613VAL Wireless Router and Voice Adapter. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

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

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

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

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

Power Light Not On

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

- Make sure that the power cord is properly connected to your router and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12V DC @ 1.2A output power adapter supplied by NETGEAR for this product.

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

Lights Never Turn Off

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

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

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.61.1. 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.

LAN or Internet (WAN) Port Lights Not On

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

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:
  - — When connecting the router's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

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

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

- Make sure your computer’s IP address is on the same subnet as the router. If you are using the default addressing schemes, your computer’s address should be in the range of 192.168.61.2 to 192.168.61.253. Refer to “Verifying TCP/IP Properties” on page C-8 or “Verifying TCP/IP Properties for Macintosh Computers” on page C-19 to find your computer’s IP address. Follow the instructions in Appendix C to configure your computer.

  Note: If your computer’s IP address is shown as 169.254.x.x, the computer is not configured correctly for your network. Recent versions of Windows and MacOS will generate and assign a 169.254.x.x IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.
- 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 URL for the router is http://www.routerlogin.net or http://www.routerlogin.com. The factory default login name is **admin** and the password is **password,** both in lower case letters. Make sure that CAPS LOCK is off when entering this information.

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

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

Troubleshooting the ISP Connection

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

To check the WAN IP address:

1. Launch your browser and select an external site such as www.netgear.com
2. Access the Main Menu of the router’s configuration at **http://www.routerlogin.net**.

3. Under the Maintenance heading, select Router Status
4. Check that an IP address is shown for the WAN Port
   If 0.0.0.0 is shown, your router has not obtained an IP address from your ISP.

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

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

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

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

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

  OR

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

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

- Your computer may not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address as described in "Install or Verify Windows Networking Components" on page C-9. Alternatively, you may configure your computer manually with DNS addresses, as explained in your operating system documentation.

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

  If your computer obtains its information from the router by DHCP, reboot the computer and verify the gateway address as described in "Install or Verify Windows Networking Components" on page C-9.

Troubleshooting a TCP/IP Network Using a Ping Utility

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

Testing the LAN Path to Your Router

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

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

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

   ```
   ping 192.168.61.1
   ```

3. Click on OK.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

   ```
   Request timed out
   ```

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

- Wrong physical connections
  - — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or Internet (WAN) Port Lights Not On" on page 8-2.
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
  - — Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

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

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

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

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

- — Check that your computer has the IP address of your router listed as the default gateway. If the IP configuration of your computer is assigned by DHCP, this information will not be visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default gateway as described in "Install or Verify Windows Networking Components" on page C-9.
- — Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- — Check that your cable or DSL modem is connected and functioning.
- — If your ISP assigned a host name to your computer, enter that host name as the Account Name in the Basic Settings menu.

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

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router’s administration password to **password**. You can erase the current configuration and restore factory defaults using the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

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

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

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

Appendix A
Technical Specifications

This appendix provides technical specifications for the WGR613VAL Wireless Router and Voice Adapter.

Network Protocol and Standards Compatibility	
Data and Routing Protocols:	TCP/IP, RIP-1, DHCP PPP over Ethernet (PPPoE)
Power Adapter	
All regions (output):	12V DC @ 1.2A output
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
Interface Specifications	The router incorporates Auto UplinkTM 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	2.4Ghz
Data Encoding:	802.11b/g 2.4GHz to 2.5GHz CCK and OFDM Modulation
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)
802.11 Security:	40-bits (also called 64-bits) and 128-bits WEP and WPA

Appendix B
Network, Routing, and Firewall 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 RFC documents for further information. An RFC is a Request For Comment (RFC) 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 *www.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 WGR613VAL Wireless Router and Voice Adapter 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 WGR613VAL 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 www.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 follow figure shows the three main address classes, including network and host sections of the address for each address type.

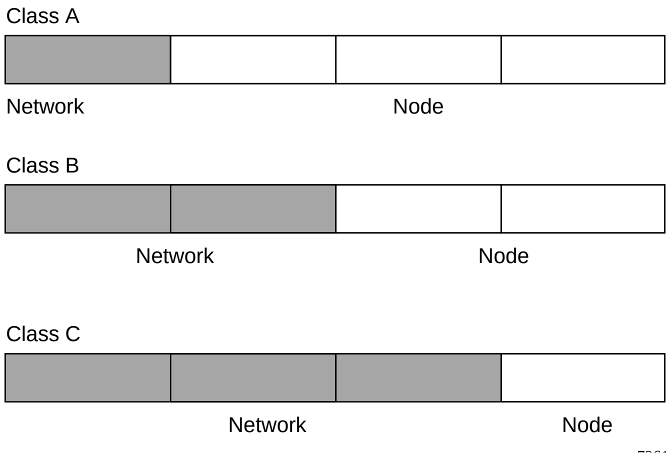


Figure B-1: Three Main Address Classes

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.

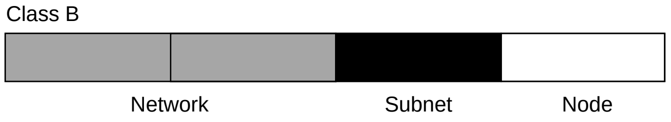


Figure B-2: Example of Subnetting a Class B Address

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 8-1. 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 8-2. 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
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 WGR613VAL 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 www.ietf.org.

Single IP Address Operation Using NAT

In the past, if multiple computers 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 WGR613VAL wireless router employs an address-sharing method called Network Address Translation (NAT). This method allows several networked computers 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.

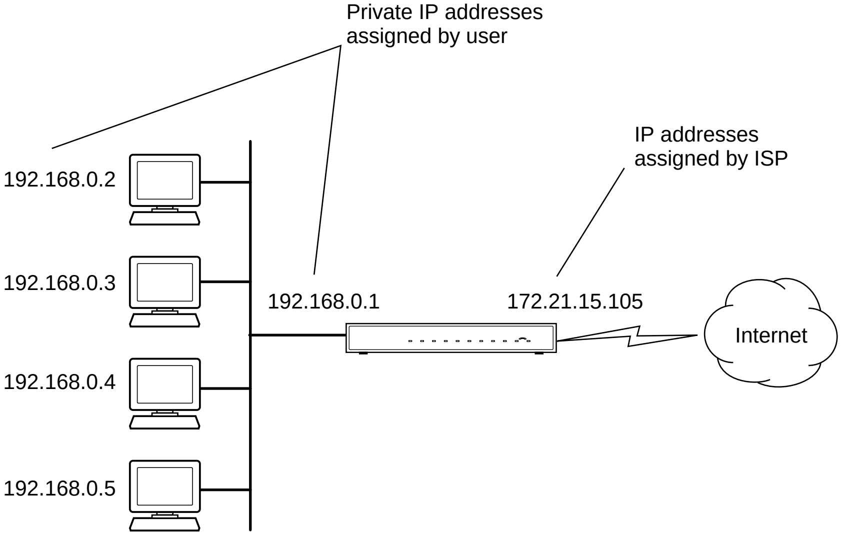


Figure B-3: Single IP Address Operation Using NAT

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 computer (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 computer accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The computer 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 computer must be configured with an IP address. If the computers 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 computer 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 WGR613VAL wireless router has the capacity to act as a DHCP server.

The WGR613VAL 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 E-mail 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

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring as described below in Table B-1.

Table B-1. 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

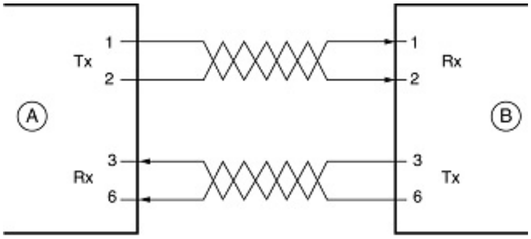
The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

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.

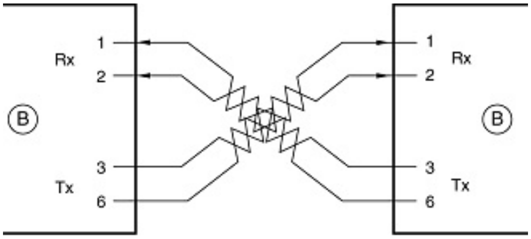
Figure B-4 illustrates straight-through twisted pair cable.



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

Figure B-5 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

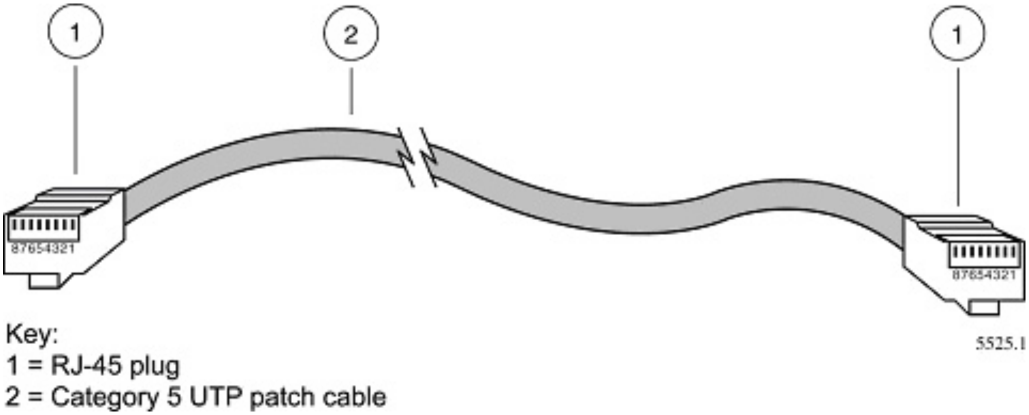


Figure B-6: Category 5 UTP Cable with Male RJ-45 Plug at Each End

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 computer, which is wired as Media Dependant Interface (MDI). In this wiring, the computer 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 computer to a computer, 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 green pairs will be exchanged from one connector to the other.

The WGR613VAL 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 computer) 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 WGR613VAL Wireless Router and Voice Adapter 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-21 or "Obtaining ISP Configuration Information for Macintosh Computers" on page C-22 for further information.

What You Need To Use a Router with a Broadband Modem

You need to prepare these three things before you begin:

Cabling and Computer Hardware

To use the WGR613VAL wireless router on your network, each computer must have an 802.11g or 802.11b wireless adapter or an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network using an Ethernet NIC at 100 Mbps, you must use a Category 5 (Cat 5) cable such as the one provided with your router. For an explanation of Ethernet cabling, see "Ethernet Cabling" on page B-11. The cable or DSL broadband modem must provide a standard 10 Mbps (10BASE-T) or 100 Mbps (100BASE-Tx) Ethernet interface.

Computer Network Configuration Requirements

The WGR613VAL includes a built-in Web Configuration Manager. To access the configuration menus on the WGR613VAL, your must use a Java-enabled Web browser program which 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 will 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 *NETGEAR Wireless Router Setup CD*, or in this appendix.

Internet Configuration Requirements

Depending on how your Internet service set up your account, you may 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 Internet service provides all the information needed to connect to the Internet. If you cannot locate this information, you can ask your Internet service to provide it or you can try one of the options below.
- If you have a computer already connected using the Internet, 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, record the settings in the TCP/IP or Network control panel.
- You may also refer to the *NETGEAR Wireless Router Setup 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, enter 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: See the configuration worksheet at "Information to Gather Before Changing Basic Wireless Settings" on page 4-6.

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 computer, 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 computer and the firewall must be assigned a unique IP addresses. Each computer 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 computer 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, and Firewall Basics."

The WGR613VAL 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—192.168.61.2 through 192.168.61.253
- Subnet mask—255.255.255.0
- Gateway address (the firewall)—192.168.61.1

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.

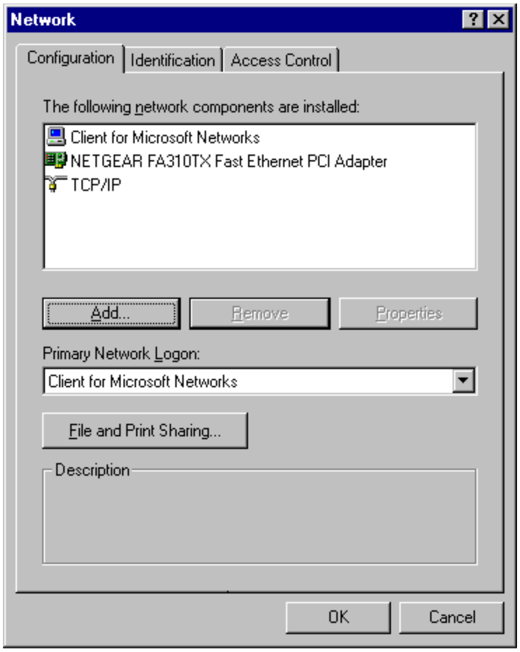
Install or Verify Windows Networking Components

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:



The following network components are installed:

Client for Microsoft Networks
NETGEAR FA310TX Fast Ethernet PCI Adapter
TCP/IP

Primary Network Logon:
Client for Microsoft Networks

   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 in Windows 95B, 98, and Me

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.

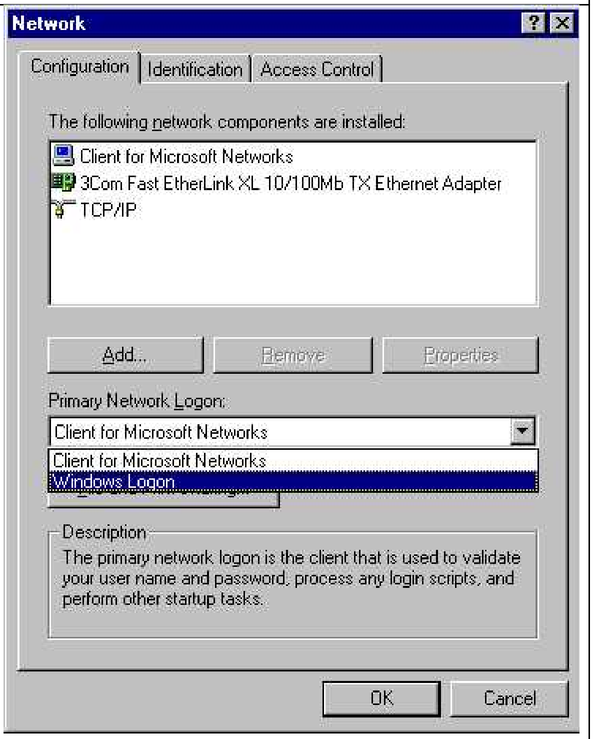
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click **Start** on the task bar located at the bottom left of the window.
  - Choose **Settings**, and then **Control Panel**.
  - 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 on the **Properties** button. The following TCP/IP Properties window will display.



The following network components are installed:

- Client for Microsoft Networks
- 3Com Fast EtherLink XL 10/100Mb TX Ethernet Adapter
- TCP/IP

Primary Network Logon:

Client for Microsoft Networks

- Client for Microsoft Networks
- Windows Logon

Description

The primary network logon is the client that is used to validate your user name and password, process any login scripts, and perform other startup tasks.

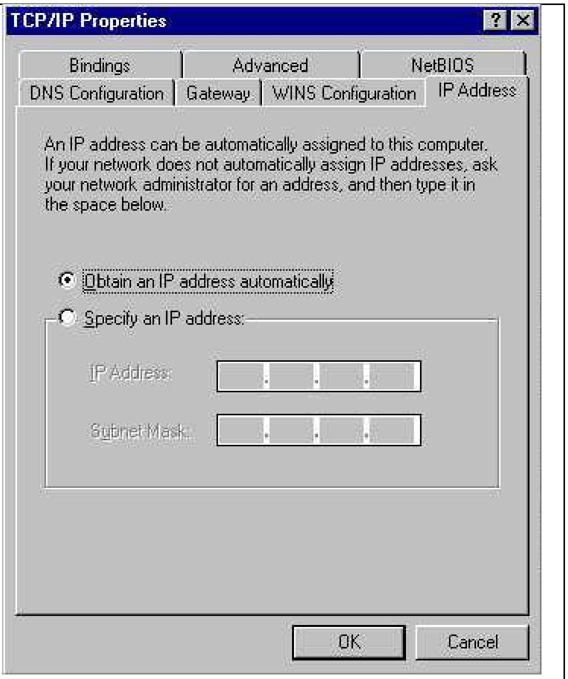
3

- 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.



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address:

Subnet Mask:

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 192.168.61.2 and 192.168.61.253
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.61.1

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

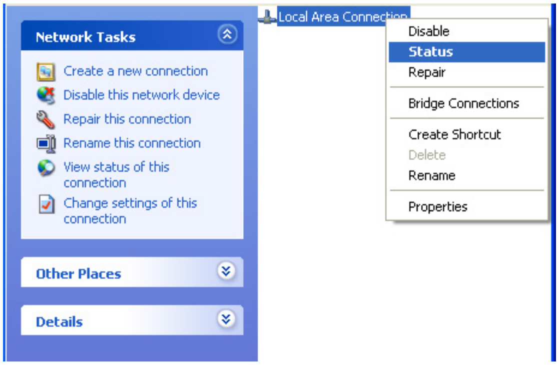
Locate your **Network Neighborhood** icon.

- 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

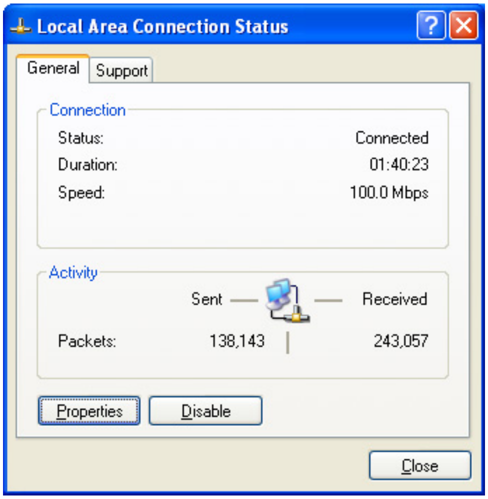
- Now the Network Connection window displays.

  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.



Local Area Connection Status

General | Support

Connection

Status: Connected

Duration: 01:40:23

Speed: 100.0 Mbps

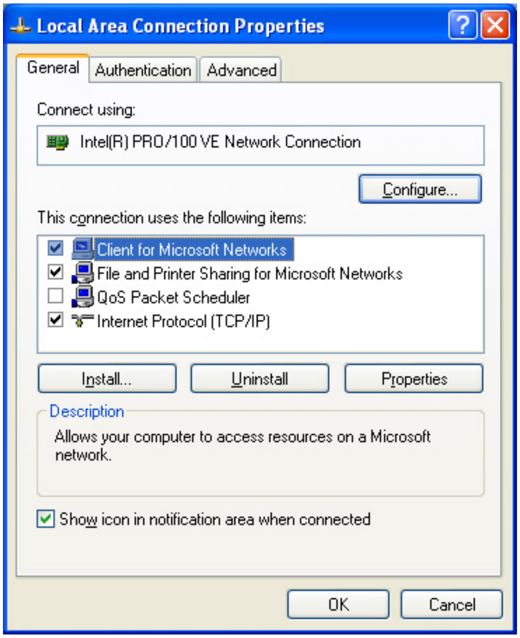
Activity

Sent — — Received

Packets: 138,143 | 243,057

4

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



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

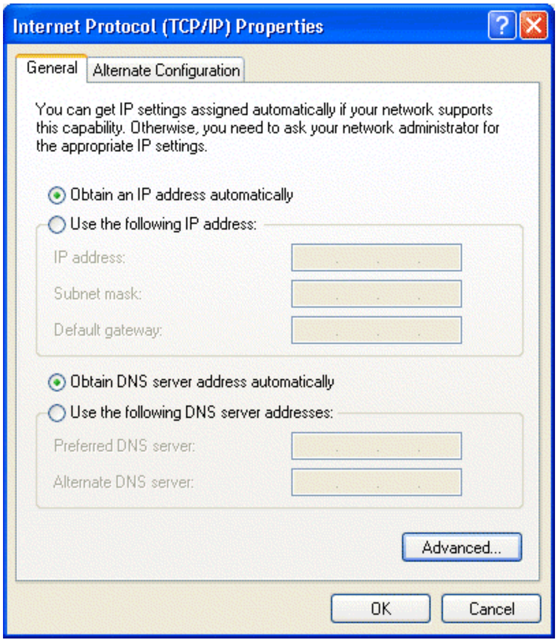
□ QoS Packet Scheduler

☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

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.	

Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

DHCP Configuration of TCP/IP in Windows 2000

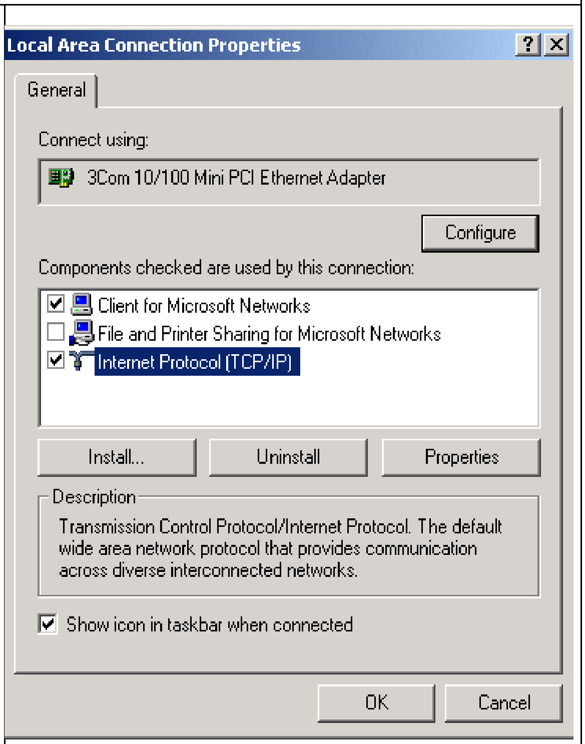
Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

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**.



Connect using:

3Com 10/100 Mini PCI Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
□ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

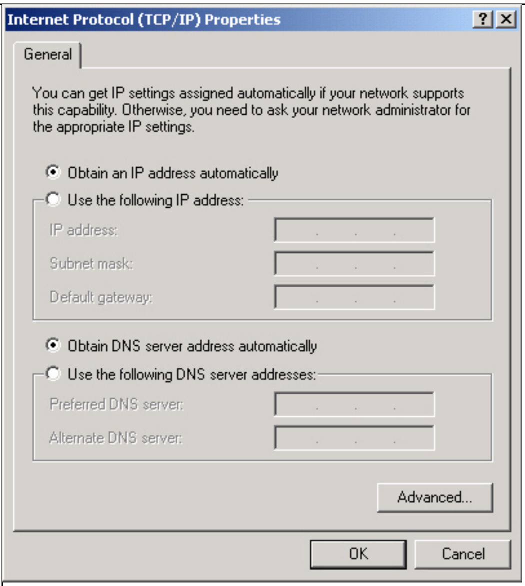
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

3

- With Internet Protocol (TCP/IP) selected, click on **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.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

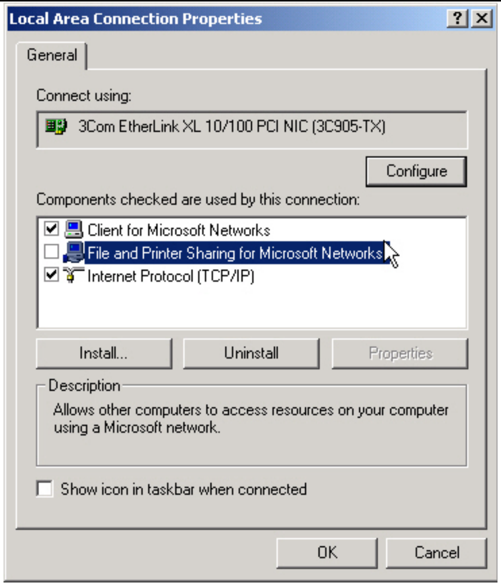
Alternate DNS server:

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.



Local Area Connection Properties

General

Connect using:

3Com EtherLink XL 10/100 PCI NIC (3C905-TX)

Components checked are used by this connection:

☑ Client for Microsoft Networks

☐ File and Printer Sharing for Microsoft Networks

☑ Internet Protocol (TCP/IP)

Description

Allows other computers to access resources on your computer using a Microsoft network.

☐ Show icon in taskbar when connected

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.

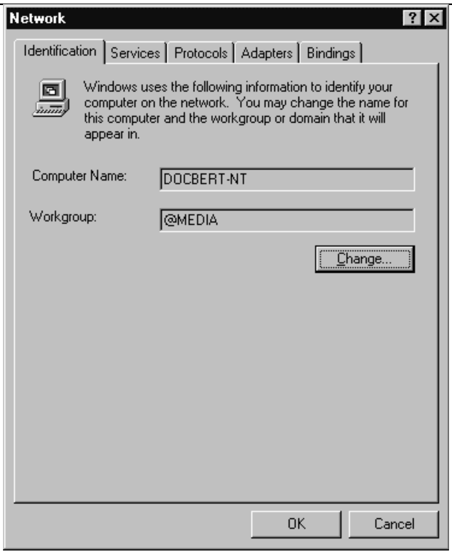
1

- 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.



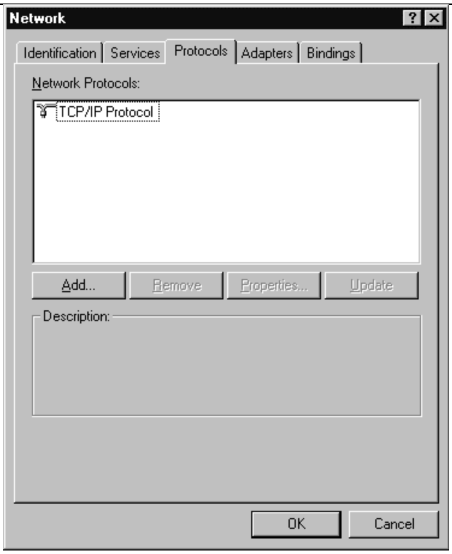
Windows uses the following information to identify your computer on the network. You may change the name for this computer and the workgroup or domain that it will appear in.

Computer Name: DOCBERT-NT

Workgroup: @MEDIA

3

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



Network

Network Protocols:

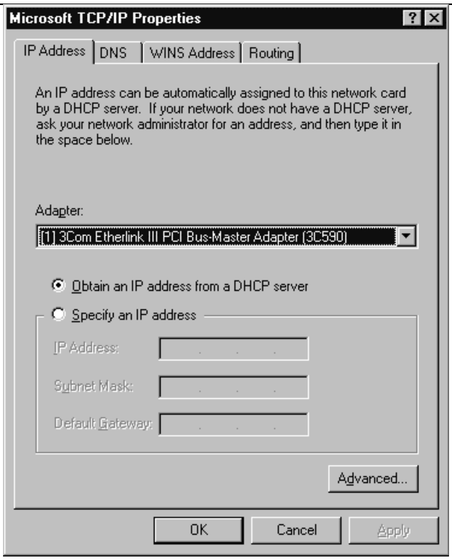
TCP/IP Protocol

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.



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter: [1] 3Com Etherlink III PCI Bus-Master Adapter (3C590)

● Obtain an IP address from a DHCP server

○ Specify an IP address

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

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 192.168.61.2 and 192.168.61.253
   - The subnet mask is 255.255.255.0

- The default gateway is 192.168.61.1

4. Type **`exit`**

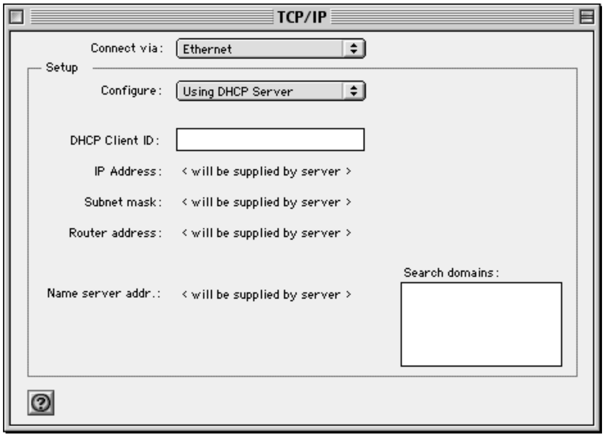
Configuring the Macintosh for TCP/IP Networking

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:



Connect via: Ethernet

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

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.

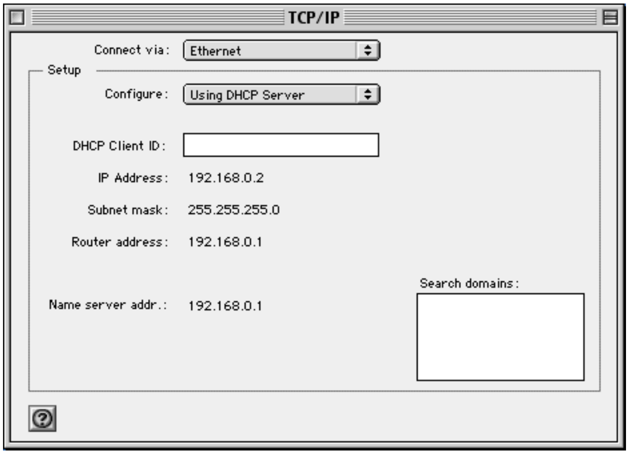
MacOS X

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.



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: 192.168.0.2

Subnet mask: 255.255.255.0

Router address: 192.168.0.1

Name server addr.: 192.168.0.1

Search domains:

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 192.168.61.2 and 192.168.61.253
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.61.1

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 WGR613VAL 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 WGR613VAL 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 router.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your WGR613VAL 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 WGR613VAL wireless router conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b and 802.11g standards for wireless LANs (WLANs). 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 802.11b 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, 54, and 108 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.

The ESSID is usually broadcast in the air from an access point. The wireless station sometimes can be configured with the ESSID **ANY.** This means the wireless station will try to associate with whichever access point has the stronger radio frequency (RF) signal, providing that both the access point and wireless station use Open System authentication.

Authentication and WEP Data Encryption

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 these two types of authentication methods:

- **Open System**. With Open System authentication, a wireless computer can join any network and receive any messages that are not encrypted.

- **Shared Key**. 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.

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 WGR613VAL:

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 below.

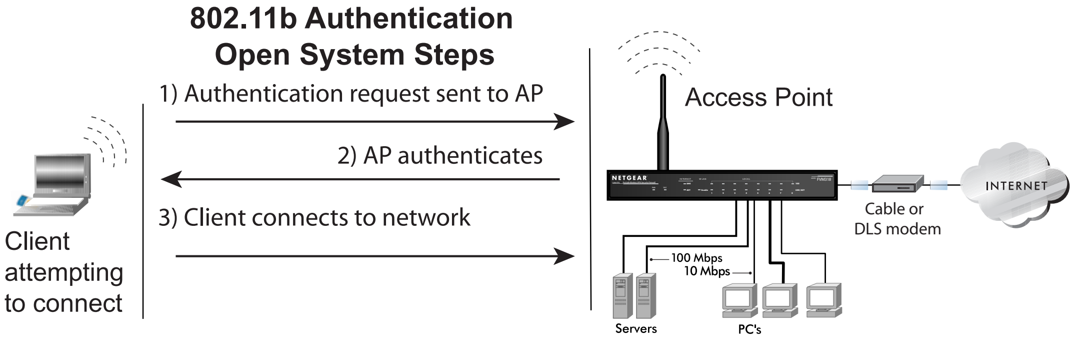


Figure D-1: Open system authentication

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 (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 below.

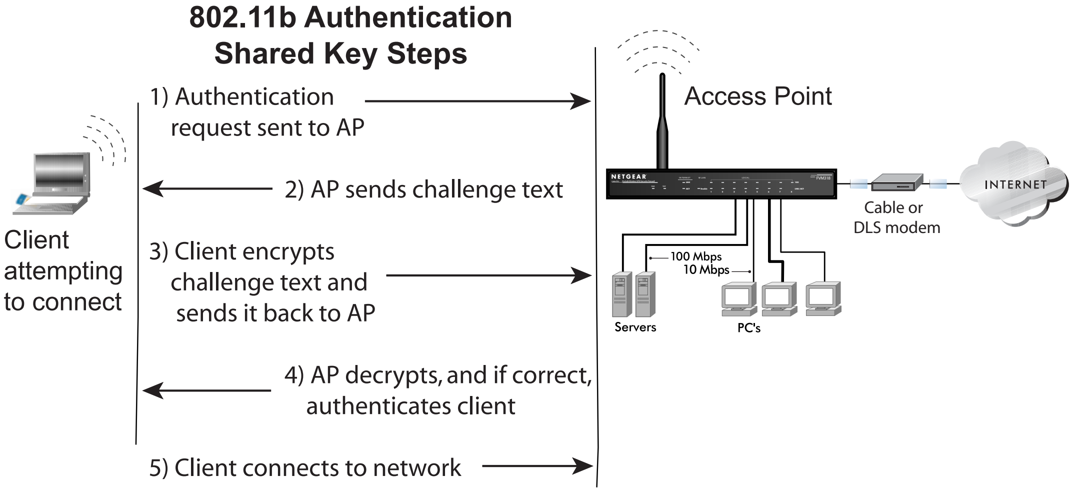

802.11b Authentication
Shared Key Steps
1) Authentication request sent to AP
2) AP sends challenge text
3) Client encrypts challenge text and sends it back to AP
4) AP decrypts, and if correct, authenticates client
5) Client connects to network
Client attempting to connect
Access Point
NETGEAR
INTERNET
Cable or DLS modem
100 Mbps
10 Mbps
Servers
PC's

Figure D-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 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 device decrypts the data using the same WEP Key. For authentication purposes, the wireless 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, 802.11 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.

Table D-3: Encryption Key Sizes

Encryption Key Size	# of Hexadecimal Digits	Example of Hexadecimal Key Content
64-bit (24+40)	10	4C72F08AE1
128-bit (24+104)	26	4C72F08AE19D57A3FF6B260037

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, and so on.

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

The wireless frequencies used by 802.11b/g networks are discussed below.

IEEE 802.11b/g 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 cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used in 802.11b/g networks are listed in Table D-4:

Table D-4: 802.11b/g 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

Table D-4: 802.11b/g Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
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. For example, Channels 1 to 11 are supported in the U.S. and Canada, and Channels 1 to 13 are supported in Europe and Australia.

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 and WPA2 Wireless Security

Wi-Fi Protected Access (WPA and WPA2) 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 that has been defined by the IEEE.

WPA and WPA2 offer the following benefits:

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

The Wi-Fi Alliance is now performing interoperability certification testing on Wi-Fi Protected Access products. Starting August of 2003, all new Wi-Fi certified products have to support WPA. NETGEAR is implementing WPA and WPA2 on client and access point products. The 802.11i standard was ratified in 2004.

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 WPA2 (IEEE 802.11i)?

WPA is forward compatible with the WPA2 security specification. WPA is a subset of WPA2 and used certain pieces of the early 802.11i draft, such as 802.1x and TKIP. The main pieces of WPA2 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 were either not yet ready for market or required hardware upgrades to implement.

What are the Key Features of WPA and WPA2 Security?

The following security features are included in the WPA and WPA2 standard:

- WPA and WPA2 Authentication
- WPA and WPA2 Encryption Key Management
  - Temporal Key Integrity Protocol (TKIP)
  - Michael message integrity code (MIC)
  - AES support (WPA2, requires hardware support)
- Support for a mixture of WPA, WPA2, and WEP wireless clients to allow a migration strategy, but mixing WEP and WPA/WPA2 is discouraged

These features are discussed below.

WPA/WPA2 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/WPA2 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/WPA2 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/WPA2 Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS

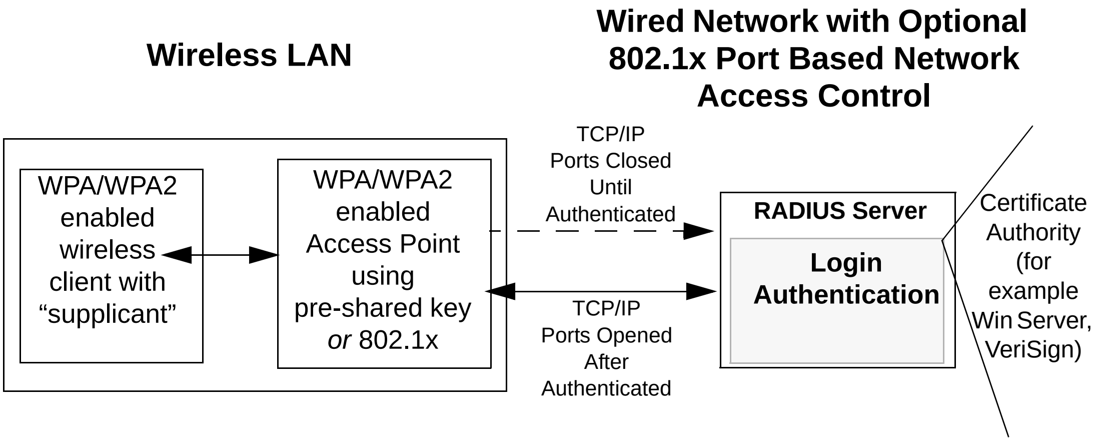

Wireless LAN
Wired Network with Optional 802.1x Port Based Network Access Control
WPA/WPA2 enabled wireless client with "supplicant"
WPA/WPA2 enabled Access Point using pre-shared key *or* 802.1x
TCP/IP Ports Closed Until Authenticated
TCP/IP Ports Opened After Authenticated
RADIUS Server
Login Authentication
Certificate Authority (for example Win Server, VeriSign)

Figure D-3: WPA/WPA2 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.

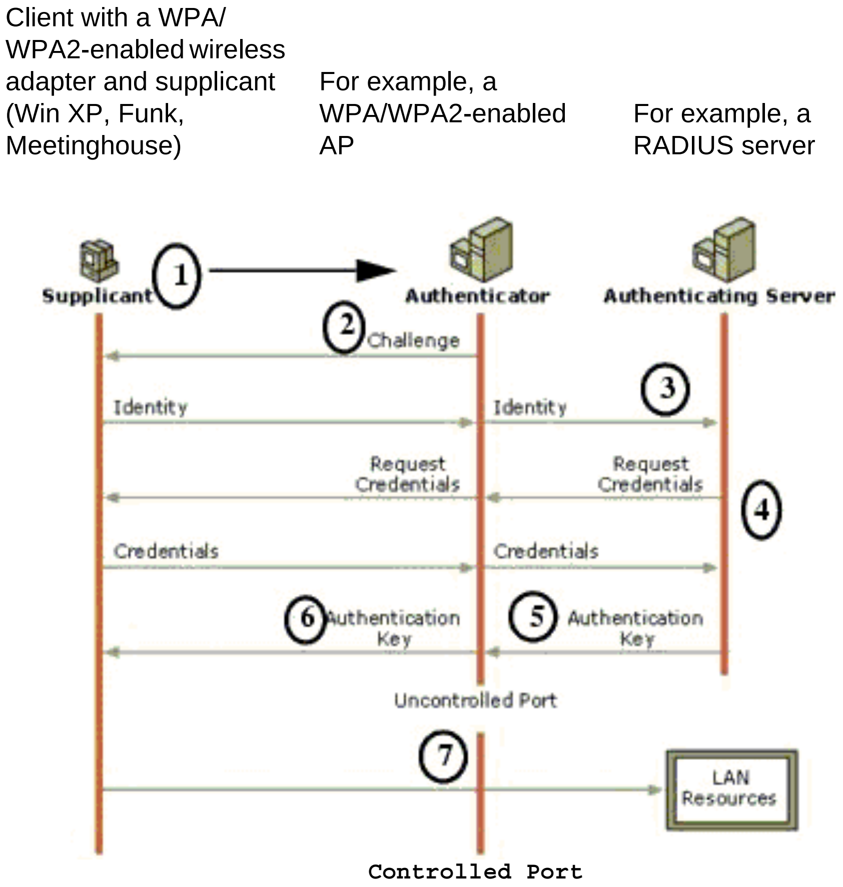


Figure D-4: 802.1x Authentication Sequence

The AP sends Beacon Frames with WPA/WPA2 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/WPA2 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/WPA2, 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.

AES Support for WPA2

One of the encryption methods supported by WPA2 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/WPA2 Perfect?

WPA/WPA2 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/WPA2 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/WPA2

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/WPA2 requires software changes to the following:

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

Supporting a Mixture of WPA, WPA2, and WEP Wireless Clients is Discouraged

To support the gradual transition of WEP-based wireless networks to WPA/WPA2, a wireless AP can support both WEP and WPA/WPA2 clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA/WPA2. The disadvantage to supporting a mixture of WEP and WPA/WPA2 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/WPA2 and non-WPA/WPA2 clients would offer network security that is no better than that obtained with a non-WPA/WPA2 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/WPA2 information element**
  To advertise their support of WPA/WPA2, wireless APs send the beacon frame with a new 802.11 WPA/WPA2 information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration information).
- **The WPA/WPA2 two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (WPA2)

To upgrade your wireless access points to support WPA/WPA2, obtain a WPA/WPA2 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/WPA2 information element**
  Wireless clients must be able to process the WPA/WPA2 information element and respond with a specific security configuration.
- **The WPA/WPA2 two-phase authentication**
  Open system, then 802.1x supplicant (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (WPA2)

To upgrade your wireless network adapters to support WPA/WPA2, obtain a WPA/WPA2 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 driver update in the wireless adapter driver. So, to update your Microsoft Windows wireless client, all you have to do is obtain the new WPA/WPA2-compatible driver and install the driver.

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA/WPA2 authentication (and preshared key) and the new WPA/WPA2 encryption algorithms (TKIP and AES).

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

Note: The Microsoft WPA2 client is still in beta.

Glossary

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

802.11 Standard

802.11, or IEEE 802.11, is a type of radio technology used for wireless local area networks (WLANs). It is a standard that has been developed by the IEEE (Institute of Electrical and Electronic Engineers), *http://standards.ieee.org*. The IEEE is an international organization that develops standards for hundreds of electronic and electrical technologies. The organization uses a series of numbers, like the Dewey Decimal system in libraries, to differentiate between the various technology families.

The 802 subgroup (of the IEEE) develops standards for local and wide area networks with the 802.11 section reviewing and creating standards for wireless local area networks.

Wi-Fi , 802.11, is composed of several standards operating in different radio frequencies: 802.11b is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps; 802.11a is a different standard for wireless LANs, and pertains to systems operating in the 5 GHz frequency range with a bandwidth of 54 Mbps. Another standard, 802.11g, is for WLANS operating in the 2.4 GHz frequency but with a bandwidth of 54 Mbps.

802.11a Standard

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.15 GHz to 5.85 GHz) with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.

802.11b Standard

International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band.

802.11d Standard

802.11d is an IEEE standard supplementary to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for client devices. The devices will automatically adjust based on geographic requirements.

The purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these countries. Equipment manufacturers do not want to produce a wide variety of country-specific products and users that travel do not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.

802.11e Standard

802.11e is a proposed IEEE standard to define quality of service (QoS) mechanisms for wireless gear that gives support to bandwidth-sensitive applications such as voice and video.

802.11g Standard

Similar to 802.11b, this physical layer standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology in order to boost overall bandwidth.

802.11i

This is the name of the IEEE Task Group dedicated to standardizing WLAN security. The 802.11i Security has a frame work based on RSN (Robust Security Mechanism). RSN consists of two parts: 1) The Data Privacy Mechanism and 2) Security Association Management.

The Data Privacy Mechanism supports two proposed schemes: TKIP and AES. TKIP (Temporal Key Integrity) is a short-term solution that defines software patches to WEP to provide a minimally adequate level of data privacy. AES or AES-OCB (Advanced Encryption Standard and Offset Codebook) is a robust data privacy scheme and is a longer-term solution.

Security Association Management is addressed by a) RSN Negotiation Procedures, b) IEEE 802.1x Authentication and c) IEEE 802.1x Key management.

The standards are being defined to naturally co-exist with pre-RSN networks that are currently deployed.

802.11n Standard

A recently formed (Oct 2003) IEEE official task group referred to as: 802.11n or "TGn" for the 100 Mbps wireless physical layer standard protocol. Current published ratification date is December 2005. As of February 2004, no draft specification has been written - It is expected to use both the 2.4 and 5GHz frequencies.

AES (Advanced Encryption Standard)

A symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. 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. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced Rhine Dahl or Rain Doll), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM. AES is expected to replace WEP as a WLAN encryption method in 2003.

Access Point (AP)

A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices. Access points can also bridge to each other.

There are various types of access points, also referred to as base stations, used in both wireless and wired networks. These include bridges, hubs, switches, routers and gateways. The differences between them are not always precise, because certain capabilities associated with one can also be added to another. For example, a router can do bridging, and a hub may also be a switch. But they are all involved in making sure data is transferred from one location to another.

A bridge connects devices that all use the same kind of protocol. A router can connect networks that use differing protocols. It also reads the addresses included in the packets and routes them to the appropriate computer station, working with any other routers in the network to choose the best path to send the packets on. A wireless hub or access point adds a few capabilities such as roaming and provides a network connection to a variety of clients, but it does not allocate bandwidth. A switch is a hub that has extra intelligence: It can read the address of a packet and send it to the appropriate computer station. A wireless gateway is an access point that provides additional capabilities such as NAT routing, DHCP, firewalls, security, etc.

Ad-Hoc mode

A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alternative set-up is one where PCs communicate with each other through an AP. See access point and Infrastructure mode.

Bandwidth

The amount of transmission capacity that is available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of users, and the type of device used to connect PCs to a network. It is similar to a pipeline in that capacity is determined by size: the wider the pipe, the more water can flow through it; the more bandwidth a network provides, the more data can flow through it. Standard 802.11b provides a bandwidth of 11 Mbps; 802.11a and 802.11g provide a bandwidth of 54 Mbps.

Bits per second (bps)

A measure of data transmission speed over communication lines based on the number of bits that can be sent or received per second. Bits per second—bps—is often confused with bytes per second—Bps. While "bits" is a measure of transmission speed, "bytes" is a measure of storage capability. 8 bits make a byte, so if a wireless network is operating at a bandwidth of 11 megabits per second (11 Mbps or 11 Mbits/sec), it is sending data at 1.375 megabytes per second (1.375 Mbps).

Bluetooth Wireless Technology

A technology specification for linking portable computers, personal digital assistants (PDAs) and mobile phones for short-range transmission of voice and data across a global radio frequency band without the need for cables or wires. Bluetooth is a frequency-hopping technology in the 2.4 GHz frequency spectrum, with a range of 30 feet and up to 11Mbps raw data throughput.

Bridge

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.

Client or Client devices

Any computer connected to a network that requests services (files, print capability) from another member of the network. Clients are end users. Wi-Fi client devices include PC Cards that slide into laptop computers, mini-PCI modules embedded in laptop computers and mobile computing devices, as well as USB and PCI/ ISA bus Wi-Fi radios. Client devices usually communicate with hub devices like access points and gateways.

Collision avoidance

A network node characteristic for proactively detecting that it can transmit a signal without risking a collision, thereby ensuring a more reliable connection.

Crossover cable

A special cable used for networking two computers without the use of a hub. Crossover cables may also be required for connecting a cable or DSL modem to a wireless gateway or access point. Instead of the signals transferring in parallel paths from one set of plugs to another, the signals "crossover." If an eight-wire cable was being used, for instance, the signal would start on pin one at one end of the cable and end up on pin eight at the other end. They "cross-over" from one side to the other.

CSMA/CA (Carrier Sense Multiple Action/Collision Avoidance)

CSMA/CA is the principle medium access method employed by IEEE 802.11 WLANs. It is a "listen before talk": method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. IEEE 802.11 states collision avoidance method rather than collision detection must be used, because the standard employs half duplex radios—radios capable of transmission or reception—but not both simultaneously.

Unlike conventional wired Ethernet nodes, a WLAN station cannot detect a collision while transmitting. If a collision occurs, the transmitting station will not receive an ACKnowledge packet from the intended receive station. For this reason, ACK packets have a higher priority than all other network traffic. After completion of a data transmission, the receive station will begin transmission of the ACK packet before any other node can begin transmitting a new data packet. All other stations must wait a longer pseudo randomized period of time before transmitting. If an ACK packet is not received, the transmitting station will wait for a subsequent opportunity to retry transmission

CSMA/CD (Carrier Sense Multiple Action/Collision Detection)

A method of managing traffic and reducing noise on an Ethernet network. A network device transmits data after detecting that a channel is available. However, if two devices transmit data simultaneously, the sending devices detect a collision and retransmit after a random time delay.

DHCP (Dynamic Host Configuration Protocol)

A utility that enables a server to dynamically assign IP addresses from a predefined list and limit their time of use so that they can be reassigned. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it.

Diversity: antenna

A type of antenna system that uses two antennas to maximize reception and transmission quality and reduce interference

DNS (Domain Name System)

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers. The program works behind the scenes to facilitate surfing the Web with alpha versus numeric addresses. A DNS server converts a name like mywebsite.com to a series of numbers like 107.22.55.26. Every website has its own specific IP address on the Internet.

Encryption Key

An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted so it can be safely shared among members of a network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.

Enhanced Data Encryption through TKIP

To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). 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 WEP known vulnerabilities.

Enterprise-level User Authentication via 802.1x and EAP

WEP has almost no user authentication mechanism. To strengthen user authentication, Wi-Fi Protected Access implements 802.1x and the Extensible Authentication Protocol (EAP). Together, these implementations provide a framework for strong user authentication. This framework utilizes a central authentication server, such as RADIUS, to authenticate each user on the network before they join it, and also employs "mutual authentication" so that the wireless user doesn’t accidentally join a rogue network that might steal its network credentials.

ESSID (more commonly referred to as SSID – Short Set Identifier)

The identifying name of an 802.11 wireless network. When you specify your correct ESSID in your client setup you ensure that you connect to your wireless network rather than another network in range. (See SSID.) The ESSID can be called by different terms, such as Network Name, Preferred Network, SSID or Wireless LAN Service Area.

Ethernet

International standard networking technology for wired implementations. Basic 10BaseT networks offer a bandwidth of about 10 Mbps. Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps) are becoming popular.

Firewall

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, hardware or a combination of both. Firewalls can prevent unrestricted access into a network, as well as restrict data from flowing out of a network.

Gateway

In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

Hot Spot (also referred to as Public Access Location)

A place where you can access Wi-Fi service. This can be for free or for a fee. HotSpots can be inside a coffee shop, airport lounge, train station, convention center, hotel or any other public meeting area. Corporations and campuses are also implementing HotSpots to provide wireless Internet access to their visitors and guests. In some parts of the world, HotSpots are known as CoolSpots.

Hub

A multiport device used to connect PCs to a network via Ethernet cabling or via Wi-Fi. Wired hubs can have numerous ports and can transmit data at speeds ranging from 10 Mbps to multigigabyte speeds per second. A hub transmits packets it receives to all the connected ports. A small wired hub may only connect 4 computers; a large hub can connect 48 or more. Wireless hubs can connect hundreds.

HZ (‘hertz”)

The international unit for measuring frequency, equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 535—1605 kHz, the FM broadcast radio frequency band is 88—108 MHz, and wireless 802.11b LANs operate at 2.4 GHz.

IEEE (Institute of Electrical and Electronics Engineers)

A membership organization (*www.ieee.org*) that includes engineers, scientists and students in electronics and allied fields. It has more than 300,000 members and is involved with setting standards for computers and communications.

IEEE 802.11

A set of specifications for LANs from The Institute of Electrical and Electronics Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5, the specification for token ring networks. 802.11 defines the standard for wireless LANs encompassing three incompatible (non-interoperable) technologies: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared. WECA's (Wireless Ethernet Compatibility Alliance – now Wi-Fi Alliance) focus is on 802.11b, an 11 Mbps high-rate DSSS standard for wireless networks.

Infrastructure mode

A client setting providing connectivity to an access point (AP). As compared to Ad-Hoc mode, whereby PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighborhood, but also provides communication with the wired network. See Ad-Hoc and AP.

IP (Internet Protocol) address

A 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network.

ISO Network Model

A network model developed by the International Standards Organization (ISO) that consists of seven different levels, or layers. By standardizing these layers, and the interfaces in between, different portions of a given protocol can be modified or changed as technologies advance or systems requirements are altered. The seven layers are:

- Physical
- Data Link
- Network
- Transport
- Session
- Presentation
- Application

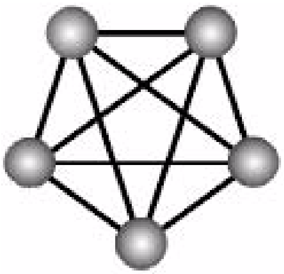
The IEEE 802.11 Standard encompasses the physical layer (PHY) and the lower portion of the data link layer. The lower portion of the data link layer is often referred to as the Medium Access Controller (MAC) sublayer.

MAC (Media Access Control)

Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.

Mesh Networks

Also called mesh topology, mesh is a network topology in which devices are connected with many redundant interconnections between network nodes. In a full mesh topology every node has a connection to every other node in the network. Mesh networks may be wired or wireless.



Mesh network

In a wireless mesh example, each of the spheres below represent a mesh router. Corporate servers and printers may be shared by attaching to each mesh router. For wireless access to the mesh, an access point must be attached to any one of the mesh routers.

Multiple Input Multiple Output (MIMO)

MIMO refers to radio links with multiple antennas at the transmitter and the receiver side to improve the performance of the wireless link.

NAT (Network Address Translation)

A network capability that enables a houseful of computers to dynamically share a single incoming IP address from a dial-up, cable or xDSL connection. NAT takes the single incoming IP address and creates new IP address for each client computer on the network.

Network name

Identifies the wireless network for all the shared components. During the installation process for most wireless networks, you need to enter the network name or SSID. Different network names are used when setting up your individual computer, wired network or workgroup.

NIC (Network Interface Card)

A type of PC adapter card that either works without wires (Wi-Fi) or attaches to a network cable to provide two-way communication between the computer and network devices such as a hub or switch. Most office wired NICs operate at 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) or 10/100 Mbps dual speed. High-speed Gigabit and 10 Gigabit NIC cards are also available. See PC Card.

PC card (also called PCMCIA)

A removable, credit-card-sized memory or I/O (input/output) device that fits into a Type 2 PCMCIA standard slot, PC Cards are used primarily in PCs, portable computers, PDAs and laptops. PC Card peripherals include Wi-Fi cards, memory cards, modems, NICs, hard drives, etc.

PCI adapter

A high-performance I/O computer bus used internally on most computers. Other bus types include ISA and AGP. PCIs and other computer buses enable the addition of internal cards that provide services and features not supported by the motherboard or other connectors.

Peer-to-peer network (also called Ad-Hoc in WLANs)

A wireless or wired computer network that has no server or central hub or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an access point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance.

PHY

The lowest layer within the OSI Network Model. It deals primarily with transmission of the raw bit stream over the PHYsical transport medium. In the case of wireless LANs, the transport medium is free space. The PHY defines parameters such as data rates, modulation method, signaling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the PHY corresponds to the radio front end and baseband signal processing sections.

Plug and Play

A computer system feature that provides for automatic configuration of add-ons and peripheral devices such as wireless PC Cards, printers, scanners and multimedia devices.

Proxy server

Used in larger companies and organizations to improve network operations and security, a proxy server is able to prevent direct communication between two or more networks. The proxy server forwards allowable data requests to remote servers and/or responds to data requests directly from stored remote server data

Range

The distance away from your access point that your wireless network can reach. Most Wi-Fi systems will provide a range of a hundred feet or more. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to mile

Residential gateway

A wireless device that connects multiple PCs, peripherals and the Internet on a home network. Most Wi-Fi residential gateways provide DHCP and NAT as well.

RJ-45

Standard connectors used in Ethernet networks. Even though they look very similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Roaming

Moving seamlessly from one AP coverage area to another with your laptop or desktop with no loss in connectivity.

Rogue Access Point

"Rogue AP" is a term used to describe an unauthorized access point that is connected on the main home or corporate network or operating in a stand-alone mode (in a parking lot or in a neighbor's building). Rogue APs, by definition, are not under the management of network administrators and do not conform to network security policies and may present a severe security risk. Ideally, it is best to have some type of WLAN system that does not allow rogue access points to easily be added to an existing WLAN.

Router

A device that forwards data packets from one local area network (LAN) or wide area network (WAN) to another. Based on routing tables and routing protocols, routers can read the network address in each transmitted frame and make a decision on how to send it via the most efficient route based on traffic load, line costs, speed, bad connections, etc.

Satellite broadband

A wireless high-speed Internet connection provided by satellites. Some satellite broadband connections are two-way—up and down. Others are one-way, with the satellite providing a high-speed downlink and then using a dial-up telephone connection or other land-based system for the uplink to the Internet.

Server

A computer that provides its resources to other computers and devices on a network. These include print servers, Internet servers and data servers. A server can also be combined with a hub or router.

Site survey

The process whereby a wireless network installer inspects a location prior to putting in a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.

SSID (also called ESSID)

A 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. (Also called ESSID.) The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet, it does not supply any security to the network. An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

SSL (Secure Sockets Layer)

Commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Switch

A type of hub that efficiently controls the way multiple devices use the same network so that each can operate at optimal performance. A switch acts as a networks traffic cop: rather than transmitting all the packets it receives to all ports as a hub does, a switch transmits packets to only the receiving port.

TCP (Transmission Control Protocol)

A protocol used along with the Internet Protocol (IP) to send data in the form of individual units (called packets) between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

For example, when a web page is downloaded from a web server, the TCP program layer in that server divides the file into packets, numbers the packets, and then forwards them individually to the IP program layer. Although each packet has the same destination IP address, it may get routed differently through the network. At the other end, TCP reassembles the individual packets and waits until they have all arrived to forward them as a single file.

TCP/IP

The underlying technology behind the Internet and communications between computers in a network. The first part, TCP, is the transport part, which matches the size of the messages on either end and guarantees that the correct message has been received. The IP part is the user's computer address on a network. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup or permanently assigned. All TCP/IP messages contain the address of the destination network as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide.

TKIP

A security feature that is a WEP enhancement: Temporal Key Integrity Protocol and Message Integrity Check (MIC) is a modification of WEP to defend against known attacks (WEP+ four patches for key mixing, message integrity, rekeying, initialization vector protection)

USB (Universal Serial Bus)

A high-speed bidirectional serial connection between a PC and a peripheral that transmits data at the rate of 12 megabits per second. The new USB 2.0 specification provides a data rate of up to 480 Mbps, compared to standard USB at only 12 Mbps. 1394, FireWire and iLink all provide a bandwidth of up to 400 Mbps.

VoIP (Voice over IP)

Voice transmission using Internet Protocol to create digital packets distributed over the Internet. VoIP can be less expensive than voice transmission using standard analog packets over POTS (Plain Old Telephone Service).

VPN (Virtual Private Network)

A type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

War Chalking

The act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot.

There are three basic designs that are currently used: a pair of back-to-back semicircles, which denotes an open node; a closed circle, which denotes a closed node; a closed circle with a “W” inside, which denotes a node equipped with WEP. Warchalkers also draw identifiers above the symbols to indicate the password that can be used to access the node, which can easily be obtained with sniffer software.

As a recent development, the debate over the legality of warchalking is still going on.

The practice stems from the U.S. Depression-era culture of wandering hobos who would make marks outside of homes to indicate to other wanderers whether the home was receptive to drifters or was inhospitable.

War Driving

War driving is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Some people have made a sport out of war driving, in part to demonstrate the ease with which wireless LANs can be compromised. With an omnidirectional antenna and a geophysical positioning system (GPS), the war driver can systematically map the locations of 802.11b wireless access points.

WEP (Wired Equivalent Privacy)

Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.

Wi-Fi (Wireless Fidelity)

Another name for IEEE 802.11b. Products certified as Wi-Fi are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

Wi-Fi Alliance (formerly WECA – Wireless Ethernet Compatibility Alliance)

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Currently the Wi-Fi Alliance has 193 member companies from around the world, and 509 products have received Wi-Fi certification since certification began in March of 2000. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability (*www.weca.net*).

Wi-Fi Protected Access (WPA)

WPA is a security technology for wireless networks that improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). In fact, WPA was developed by the networking industry in response to the shortcomings of WEP.

One of the key technologies behind WPA is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the encryption weaknesses of WEP. Another key component of WPA is built-in authentication that WEP does not offer. With this feature, WPA provides roughly comparable security to VPN tunneling with WEP, with the benefit of easier administration and use. This is similar to 802.1x support and requires a RADIUS server in order to implement. The Wi-Fi Alliance will call this, 'WPA-Enterprise.'

One variation of WPA is called WPA Pre Shared Key or WPA-PSK for short - this provides an authentication alternative to an expensive RADIUS server. WPA-PSK is a simplified but still powerful form of WPA most suitable for home Wi-Fi networking. To use WPA-PSK, a person sets a static key or "passphrase" as with WEP. But, using TKIP, WPA-PSK automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them. The Wi-Fi Alliance will call this, 'WPA-Personal.'

Wi-Fi Protected Access and IEEE 802.11i Comparison

Wi-Fi Protected Access will be forward-compatible with the IEEE 802.11i security specification currently under development by the IEEE. Wi-Fi Protected Access is a subset of the current 802.11i draft, taking certain pieces of the 802.11i draft that are ready to bring to market today, such as its implementation of 802.1x and TKIP. These features can also be enabled on most existing Wi-Fi CERTIFIED products as a software upgrade. The main pieces of the 802.11i draft that are not included in Wi-Fi Protected Access are secure IBSS, secure fast handoff, secure de-authentication and disassociation, 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.

Wi-Fi Protected Access for the Enterprise

Wi-Fi Protected Access effectively addresses the WLAN security requirements for the enterprise and provides a strong encryption and authentication solution prior to the ratification of the IEEE 802.11i standard. In an enterprise with IT resources, Wi-Fi Protected Access should be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. With this implementation in place, the need for add-on solutions such as VPNs may be eliminated, at least for the express purpose of securing the wireless link in a network.

Wi-Fi Protected Access for Home/SOHO

In a home or Small Office/ Home Office (SOHO) environment, where there are no central authentication servers or EAP framework, Wi-Fi Protected Access runs in a special home mode. This mode, also called Pre-Shared Key (PSK), allows the use of manually-entered keys or passwords and is designed to be easy to set up for the home user. All the home user needs to do is enter a password (also called a master key) in their access point or home wireless gateway and each PC that is on the Wi-Fi wireless network. Wi-Fi Protected Access takes over automatically from that point. First, the password allows only devices with a matching password to join the network, which keeps out eavesdroppers and other unauthorized users. Second, the password automatically kicks off the TKIP encryption process, described above.

Wi-Fi Protected Access for Public Access

The intrinsic encryption and authentication schemes defined in Wi-Fi Protected Access may also prove useful for Wireless Internet Service Providers (WISPs) offering Wi-Fi public access in "hot spots" where secure transmission and authentication is particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections.

Wi-Fi Protected Access in "Mixed Mode" Deployment

In a large network with many clients, a likely scenario is that access points will be upgraded before all the Wi-Fi clients. Some access points may operate in a "mixed mode", which supports both clients running Wi-Fi Protected Access and clients running original WEP security. While useful for transition, the net effect of supporting both types of client devices is that security will operate at the less secure level (WEP), common to all the devices. Therefore, organizations will benefit by accelerating the move to Wi-Fi Protected Access for all Wi-Fi clients and access points.

WiMAX

An IEEE 802.16 Task Group that provides a specification for fixed broadband wireless access systems employing a point-to-multipoint (PMP) architecture. Task Group 1 of IEEE 802.16 developed a point-to-multipoint broadband wireless access standard for systems in the frequency range 10-66 GHz. The standard covers both the Media Access Control (MAC) and the physical (PHY) layers.

Wireless Multimedia (WMM)

WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video, audio, or voice will have a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.

Wireless Networking

Wireless Networking refers to the infrastructure enabling the transmission of wireless signals. A network ties things together and enables resource sharing.

WLAN (Wireless LAN)

Also referred to as LAN. A type of local-area network that uses wireless or high-frequency radio waves rather than wires to communicate between nodes.