Reference Manual for the Model DG824M Wireless ADSL Modem Gateway

NETGEAR

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

SM-DG824MNA-0
November 2002

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.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

EN 55 022 Declaration of Conformance

This is to certify that the DG824M Wireless ADSL Modem Gateway 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 DG824M Wireless ADSL Modem Gateway 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 DG824M Wireless ADSL Modem Gateway 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 DG824M Wireless ADSL Modem Gateway.

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.

iv

Contents

Contents   vii

Appendix A
Technical Specifications

Appendix B
Network and Routing Basics

Appendix C
Preparing Your Network

Contents

List of Procedures

2

Preface
About This Guide

Thank you for purchasing the NETGEAR™ DG824M Wireless ADSL Modem Gateway.

Audience

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and wireless technologies tutorial information is provided in the Appendices.

Technical Support

For help with any technical issues, contact Customer Support at 1-888-NETGEAR, or visit us on the Web at www.NETGEAR.com. The NETGEAR Web site includes an extensive knowledge base, answers to frequently asked questions, and a means for submitting technical questions online.

We recommend you register your product online at: www.NETGEAR.com/register

Typographical Conventions

This guide uses the following typographical conventions:

italics	Book titles and UNIX file, command, and directory names.
courier font	Screen text, user-typed command-line entries.
Initial Caps	Menu titles and window and button names.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]+C	Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.
ALL CAPS	DOS file and directory names.

Special Message Formats

This guide uses the following formats to highlight special messages:

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

Procedure: This format is used to let you know that you are following a sequence of steps required to complete a task.

Warning: This format is used to highlight information about the possibility of injury or equipment damage.

Danger: This format is used to alert you that there is the potential for incurring an electrical shock if you mishandle the equipment.

This chapter describes the features of the NETGEAR DG824M Wireless ADSL Modem Gateway. The DG824M gateway is a combination of a built-in ADSL modem, router, 4-port switch, and firewall which enables your entire network to safely share an Internet connection that otherwise is used by a single PC.

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

About the Gateway

The DG824M Wireless ADSL Modem Gateway provides continuous, high-speed 11 Mbps access between your wireless and Ethernet devices. The DG824M gateway enables your entire network to share an Internet connection through the built-in ADSL modem that otherwise is used by a single PC. With minimum setup, you can install and use the gateway within minutes.

The DG824M gateway provides multiple Web content filtering options, plus e-mail browsing activity reporting and instant alerts. Parents and network administrators can establish restricted access policies based on time-of-day, website addresses and address keywords, and share high-speed ADSL Internet access for up to 253 personal computers. The included firewall and Network Address Translation (NAT) features protect you from hackers.

Key Features

The DG824M gateway provides the following features:

• A Powerful, True Firewall

- 802.11b Standards-based wireless networking

- Content Filtering

- Auto Sensing and Auto Uplink™ LAN Ethernet Connections

- Extensive Internet Protocol Support

- Easy, web-based setup for installation and management

- A built-in ADSL modem

These features are discussed below.

802.11b Standards-based Wireless Networking

The DG824M gateway includes an 802.11b-compliant wireless access point, providing continuous, high-speed 11 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11b Standards-based wireless networking at up to 11 Mbps

- 64-bit and 128-bit WEP encryption security

- WEP keys can be generated manually or by passphrase

- Wireless access can be restricted by MAC address.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the DG824M is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection
  Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.

- Blocks unwanted traffic from the Internet to your LAN.

- Blocks access from your LAN to Internet locations or services that you specify as off-limits.

- Logs security incidents
  The DG824M will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the gateway to email the log to you at specified intervals. You can also configure the gateway to send immediate alert messages to your email address or email pager whenever a significant event occurs.

Content Filtering

With its content filtering feature, the DG824M prevents objectionable content from reaching your PCs. The gateway allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the gateway to log and report attempts to access objectionable Internet sites.

Auto Sensing and Auto Uplink™ LAN Ethernet Connections

With its internal 4-port 10/100 switch, the DG824M can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The local LAN ports are autosensing and capable of full-duplex or half-duplex operation.

The gateway incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a 'normal' connection such as to a PC or an 'uplink' connection such as to a switch or hub. That port 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.

Protocol Support

The DG824M supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). Appendix B, "Network and Routing Basics" provides further information on TCP/IP.

- IP Address Sharing by NAT
  The DG824M allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.

- Automatic Configuration of Attached PCs by DHCP
  The DG824M dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

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

- PPP over Ethernet (PPPoE)
  PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an ADSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.

- PPP over ATM (PPPoA)
  PPP over ATM is a protocol for connecting remote hosts to the Internet over an ADSL connection by simulating a ATM connection.

- Dynamic DNS
  Dynamic DNS services allow remote users to find your network using a domain name when your IP address is not permanently assigned. The gateway contains a client that can connect to many popular Dynamic DNS services to register your dynamic IP address.

Easy Installation and Management

You can install, configure, and operate the DG824M within minutes after connecting it to the network. The following features simplify installation and management tasks:

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

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

- Remote management
  The gateway allows you to login to the Web Management Interface from a remote location via the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.

- Diagnostic functions
  The gateway incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the gateway. You can use these diagnostic functions directly from the DG824M when your are connect on the LAN or when you are connected over the Internet via the remote management function.

- Visual monitoring
  The gateway's front panel LEDs provide an easy way to monitor its status and activity.

- Flash EPROM for firmware upgrade

What's in the Box?

The product package should contain the following items:

- DG824M Wireless ADSL Modem Gateway
- AC power adapter (varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable
- Microfilters (quantity and type vary by region)
- *Model DG824M Resource CD*, including:
  — This guide
  — Application Notes
- A Quick Printed Installation Guide
- Warranty and Support Information Cards

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

The Gateway's Front Panel

The DG824M Wireless ADSL Modem Gateway front panel shown below contains status LEDs.
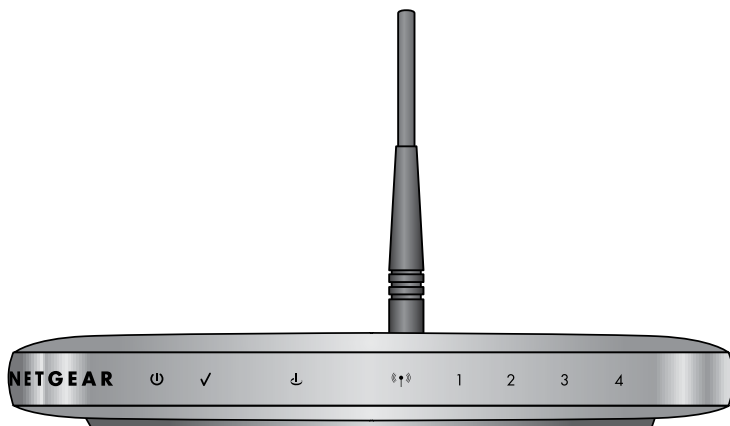
Figure 1-1: DG824M Front Panel

You can use the LEDs to verify various conditions. Table 1-1 lists and describes each LED on the front panel of the router. These LEDs are green when lit.

Table 1-1.   LED Descriptions

Label	Activity	Description
Power	On Off	Power is supplied to the router. Power is not supplied to the router.
Test	On Off	The system is initializing. The system is ready and running.
Internet	Blink -- Amber On -- Green Blink -- Green	Indicates ADSL training. The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
Wireless	On	Indicates that the Wireless port is initialized.
LAN 4	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The Local port has detected link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected on this port.

The Gateway's Rear Panel

The rear panel of the DG824M Wireless ADSL Modem Gateway (Figure 1-2) contains port connections.
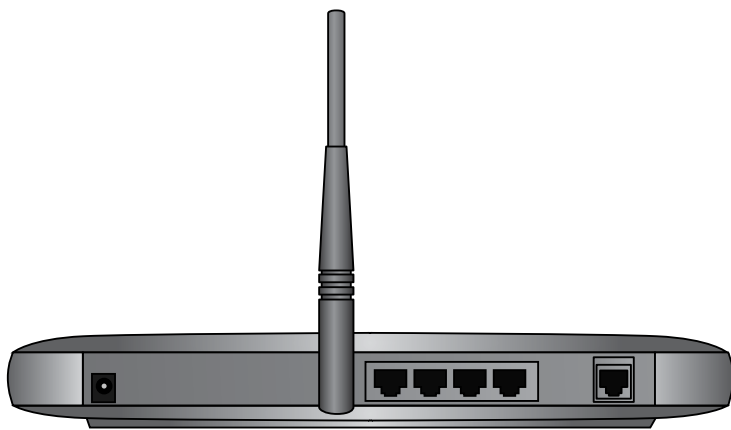
Figure 1-2: DG824M Rear Panel

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

- AC power adapter outlet

- Factory Default Reset push button

- Wireless antenna

- Four Local Ethernet RJ-45 ports for connecting the gateway to the local computers

- ADSL port for connecting the gateway to an ADSL line

Chapter 2
Connecting the Gateway to the Internet

This chapter describes how to set up the gateway on your Local Area Network (LAN), connect to the Internet, how to configure your DG824M Wireless ADSL Modem Gateway for Internet access using the Setup Wizard, or how to manually configure your Internet connection.

What You Will Need Before You Begin

You need to prepare these three things before you can establish an Internet connection through your gateway:

1. The gateway connected to an ADSL line and a computer properly connected to the gateway as explained below.

2. Active Internet service such as that provided by an ADSL account.

3. The Internet Service Provider (ISP) configuration information for your DSL account.

Cabling Requirements

The built-in ADSL modem of the DG824M gateway connects to the Internet via your telephone line using standard twisted-pair telephone cables.

Note: Do not connect the DG824M to the ADSL line through a microfilter unless the microfilter is specifically designed for this purpose. Doing so will prevent the built-in DSL modem in the DG824M from establishing a connection to the Internet. If you have any doubts about this, it is recommended that you connect the DG824 directly to the ADSL line.

The DG824M gateway connects to your LAN via twisted-pair Ethernet cables.

Computer Hardware Requirements

To use the DG824M gateway on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable, or a 802.11b wireless adapter. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your gateway.

LAN Configuration Requirements

For the initial connection to the Internet and configuration of your gateway, you will need to connect a computer to the gateway which is set to automatically get its TCP/IP configuration from the gateway via DHCP.

Note: Please refer to Appendix C, "Preparing Your Network for assistance with DHCP configuration.

Internet Configuration Requirements

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

• VPI/VCI parameters

• Multiplexing Method

• Host and Domain Names

• ISP Login Name and Password

• ISP Domain Name Server (DNS) Addresses

• Fixed or Static IP Address

Where Do I Get the Internet Configuration Parameters?

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

• Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.

• If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.

- For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties.
- For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties.
- For Macintosh computers, open the TCP/IP or Network control panel.

- You may also refer to the *DG824M Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below according to the instructions in "Record Your Internet Connection Information" on page 2-4.

Procedure 2-1: Record Your Internet Connection Information

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

ISP Multiplexing Method and Virtual Circuit Number: The default settings of your DG824M Wireless ADSL Modem Gateway will work fine for most ISPs. However, some ISPs use a specific Multiplexing Method or a Virtual Circuit Number for either the VPI or VCI. If your ISP provided you with a specific Multiplexing Method or VPI/VCI number, then fill in the following:

Multiplexing Method, circle one: LLC-based or VC-based
VPI: _____ A number between 0 and 255. VCI: _____ A number between 1and 65535.

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

Login Name: _____ Password: _____

Service Name: _____

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

Fixed or Static Internet IP Address: _____ . _____ . _____ . _____
Gateway IP Address: _____ . _____ . _____ . _____
Subnet Mask: _____ . _____ . _____ . _____

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

Primary DNS Server IP Address: _____ . _____ . _____ . _____

Secondary DNS Server IP Address: _____ . _____ . _____ . _____

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

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

ISP Host Name: _____ ISP Domain Name: _____

Connecting the DG824M Wireless ADSL Modem Gateway to Your LAN

This section provides instructions for connecting the DG824M gateway.

Note: The Resource CD included with your gateway contains an animated Installation Assistant to help you through this procedure.

Procedure 2-2: Connecting the Gateway

There are three steps to connecting your firewall:

1. Connect the gateway to your ADSL line
1. Connect the gateway to the computers on your network
2. Log in to the gateway
3. Connect to the Internet

Follow the steps below to connect your gateway to your network. You can also refer to the Resource CD included with your gateway which contains an animated Installation Assistant to help you through this procedure.

1. **Connect the DG824M.**

   a. Turn off your computer.

   b. Connect the cable (**A**) from the DG824M ADSL port to your ADSL outlet, being sure to properly connect the wires as shown in the illustration below.
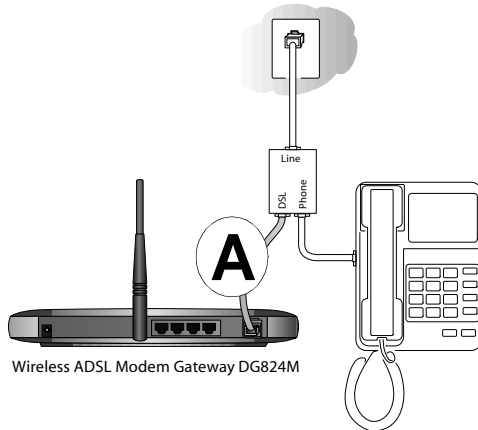
Figure 2-1: Connect the ADSL Cable

Note: The illustration above depicts a microfilter splitter specifically designed to enable a phone and ADSL modem to connect to the same phone line wall jack outlet. Do not connect the DG824B to your ADSL line with a microfilter unless the microfilter specifically designed for that purpose. Doing so will prevent the modem from establishing a connection to the Internet. If you have any doubts about this, use only a phone cord to connect the DG824B to the ADSL wall jack outlet.

c. Connect the Ethernet cable (B) from your DG824M's LAN port to a computer.
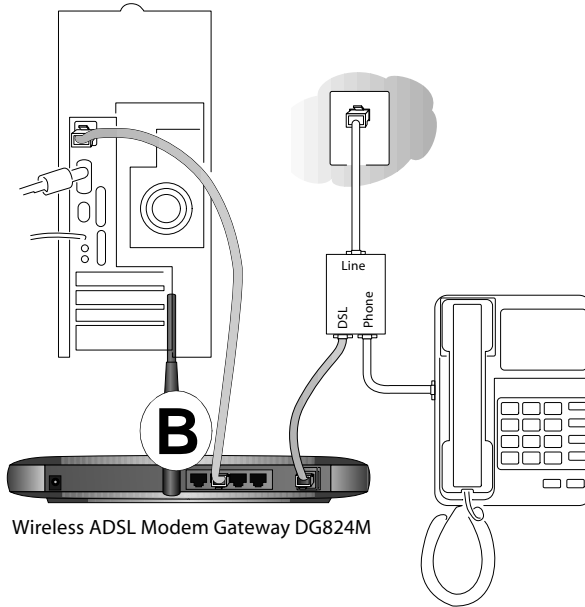
Figure 2-2: Connect the gateway to a computer

Note: The DG824M gateway incorporates Auto Uplink™ technology. Each Ethernet LAN port will automatically sense whether the cable plugged into the port should have a 'normal' connection (e.g. connecting to a PC) or an 'uplink' connection (e.g. connecting to a 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.

d. Connect the power adapter to the gateway and plug it in to a power outlet. Verify the following:

⏻ The power light is lit after turning on the gateway.

⭍ The ADSL link light is solid green, indicating a link has been established to the cable network.

e. Now, turn on your computer. If software usually logs you in to your Internet connection, do not run that software or cancel it if it starts automatically.

4 The local lights are lit for any connected computers.

Note: For instructions on connecting computers to the DG824M via wireless links, please see the Chapter 3, "Wireless Configuration".

2. Log in to the DG824M.

Note: If you usually run software to log in to your Internet connection, do not run that software.

a. Connect to the gateway by typing *http://192.168.0.1* in the address field of Internet Explorer or Netscape® Navigator.
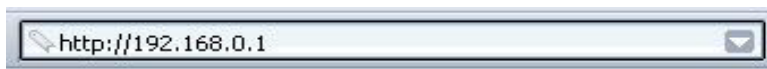
Figure 2-3: Log in to the gateway

A login window opens as shown below:
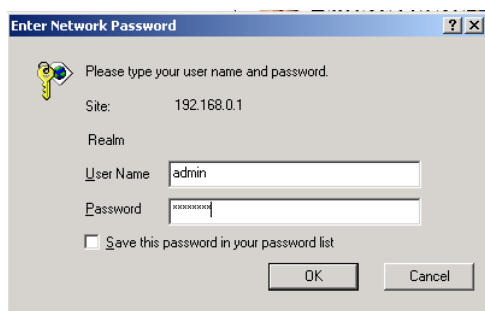
Figure 2-4: Login window

b. For security reasons, the gateway has its own user name and password. When prompted, enter **admin** for the gateway User Name and **password** for the gateway Password, both in lower case letters.

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

3.   **Connect to the Internet**.

Setup Wizard

Setup Wizard

System Can Now Detect The Connection Type Of WAN Port, Or You Can Configure It By Yourself.

Do You Want System To Detect The Connection Type?

⊙ Yes.

○ No. I Want To Configure By Myself.
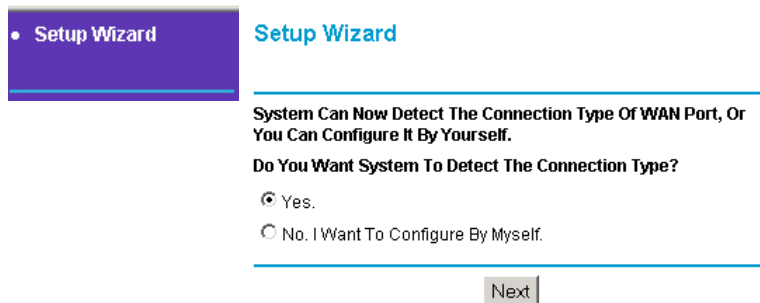
[Next]

Figure 2-5: Setup Wizard

a.   You are now connected to the gateway. If you do not see the menu above, click the Setup Wizard link on the upper left of the main menu. Click the Yes button in the *Setup Wizard*.

b.   Please click Next to follow the steps in the Setup Wizard to input the configuration parameters from your ISP to connect to the Internet.

Note: If you were unable to connect to the gateway, please refer to troubleshooting procedures in "Basic Functioning" on page 7-1.

4.   **Connect an ADSL microfilter to your phone.**

a.   ADSL transmissions use your phone wires and can interfere with the quality of your phone service. A microfilter eliminates such problems. Depending on the country of purchase, a microfilter may be included in your DG824M package. Locate a suitable microfilter.

b.   Connect the microfilter to your phone line between the phone set and the phone line wall outlet. Each phone set requires a microfilter.

Note: Improperly connecting a microfilter to your DG824M gateway will block your ADSL connection.

Connecting the DG824M to the Internet

The gateway is now properly attached to your network. You are now ready to configure your gateway to connect to the Internet. There are two ways you can configure your gateway to connect to the Internet:

- Let the DG824M auto-detect the type of Internet connection you have and configure it.

- Manually choose which type of Internet connection you have and configure it.

These options are described below. In either case, unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP you recorded in "Record Your Internet Connection Information" on page 2-4.

Procedure 2-3: Auto-Detecting Your Internet Connection Type

The Web Configuration Manager built in to the gateway contains a Setup Wizard that can automatically determine your network connection type.

1. If your gateway has not yet been configured, the Setup Wizard shown in Figure 2-6 should launch automatically.

   Note: If, instead of the Setup Wizard menu, the main menu of the gateway's Configuration Manager as shown in Figure 2-11 appears, click the Setup Wizard link in the upper left to bring up this menu.

   When the Wizard launches, select Yes in the menu below to allow the gateway to automatically determine your connection.
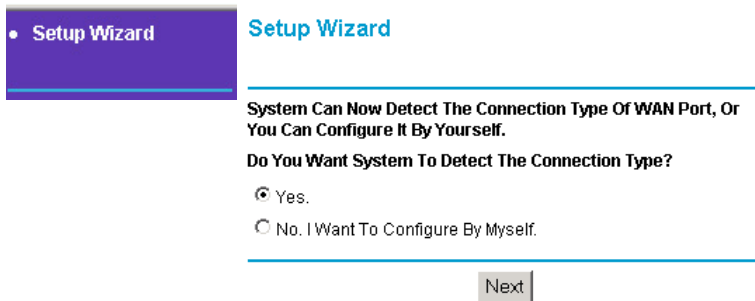
Figure 2-6: Built-in Web-based Configuration Manager Setup Wizard

2. Click Next

   The Setup Wizard will now check for the following connection types:

   - Dynamic IP assignment

   - A login protocol such as PPPoE or PPPoA

- Fixed IP address assignment

Next, the Setup Wizard will report which connection type it has discovered, and then display the appropriate configuration menu. If the Setup Wizard finds no connection, you will be prompted to check the physical connection between your gateway and the ADSL line. When the connection is properly made, the gateway's Internet LED should be on.

The procedures for filling in the configuration menu for each type of connection follow below.

Procedure 2-4: Wizard-Detected PPPoE Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over Ethernet (PPPoE), you will be directed to a menu like the PPPoE menu in Figure 2-7:

Figure 2-7: Setup Wizard menu for PPPoE login accounts

1. Enter the PPPoE login user name, password, and Service Name (if required) as provided by your ISP. These fields are case sensitive.

2. If you wish to change the login timeout, enter a new value in minutes. This determines how long the gateway keeps the Internet connection active after there is no Internet activity from the LAN. Entering a timeout value of zero means never log out.

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

3. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the gateway 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.

    If you enter an address here, after you finish configuring the gateway, reboot your PCs so that the settings take effect.

4. Click on Apply to save your settings.

5. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, "Troubleshooting".

Procedure 2-5: Wizard-Detected PPPoA Login Account Setup

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over ATM (PPPoA), you will be directed to a menu like the PPPoA menu in Figure 2-7:

Figure 2-8: Setup Wizard menu for PPPoA login accounts

1. Enter your Login and Password. These fields are case sensitive. If you wish to change the login timeout, enter a new value in minutes. This determines how long the gateway keeps the Internet connection active after there is no Internet activity from the LAN. Entering a timeout value of zero means never log out.

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

2. Domain Name Server (DNS) Address:
   These parameters may be necessary to access your ISP's services such as mail or news servers. If you leave the Domain Name field blank, the gateway will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.

   If you know that your ISP does not automatically transmit DNS addresses to the gateway 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.

   If you enter an address here, after you finish configuring the gateway, reboot your PCs so that the settings take effect.

3. Click on Apply to save your settings.

4. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, "Troubleshooting".

Procedure 2-6: Wizard-Detected Dynamic IP Account Setup

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the menu shown in Figure 2-9 below:

Dynamic IP

Account Name (If Required)	[ ]
Domain Name (If Required)	[ ]

Domain Name Server (DNS) Address
- ⦿ Get Automatically From ISP
- ○ Use These DNS Servers

    Primary DNS   [0].[0].[0].[0]
    Secondary DNS   [0].[0].[0].[0]

Router's MAC Address
- ⦿ Use Default Address
- ○ Use This MAC Address

    [Apply] [Cancel] [Test]

Figure 2-9: Setup Wizard menu for Dynamic IP address

1. 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. If you leave the Domain Name field blank, the gateway will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.

2. If you know that your ISP does not automatically transmit DNS addresses to the gateway 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.

   A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your gateway during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the gateway.

3. The Router's MAC Address is the Ethernet MAC address that will be used by the gateway on the Internet port.

If your ISP allows access from only one specific computer's Ethernet MAC address, select "Use this MAC address." The gateway 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. Otherwise, you can type in a MAC address.

> **Note:** Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your gateway to masquerade as that PC by using its MAC address.

4. Click on Apply to save your settings.

5. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, "Troubleshooting"".

Procedure 2-7: Wizard-Detected Fixed IP (Static) Account Setup

If the Setup Wizard determines that your Internet service account uses Fixed IP assignment, you will be directed to the menu shown in Figure 2-10 below:

Figure 2-10: Setup Wizard menu for Fixed IP address

1. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP's gateway router. This information should have been provided to you by your ISP. You will need the configuration parameters from your ISP you recorded in "Record Your Internet Connection Information" on page<$chapnum>4.

2. Enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

    A DNS servers are required to perform the function of translating an Internet name such as www.netgear.com to a numeric IP address. For a fixed IP address configuration, you must obtain DNS server addresses from your ISP and enter them manually here. You should reboot your PCs after configuring the gateway for these settings to take effect.

3. Click on Apply to save the settings.

4. Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to Chapter 7, "Troubleshooting".

Testing Your Internet Connection

After completing the Internet connection configuration, your can test your Internet connection. Log in to the gateway, then, from the Setup Basic Settings link, click on the Test button. If the NETGEAR website does not appear within one minute, refer to Chapter 7, "Troubleshooting".

Your gateway is now configured to provide Internet access for your network. Your gateway automatically connects to the Internet when one of your computers requires access. It is not necessary to run a dialer or login application such as Dial-Up Networking or Enternet to connect, log in, or disconnect. These functions are performed by the gateway as needed.

To access the Internet from any computer connected to your gateway, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the gateway's Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

The following chapters describe how to configure the Advanced features of your gateway, and how to troubleshoot problems that may occur.

Manually Configuring Your Internet Connection

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

Basic Settings

Does Your Internet Connection Require A Login?

⊙ No

○ Yes

| Account Name (If Required) | DG824 |
| Domain Name (If Required) | |

Internet IP Address

⊙ Get Dynamically From ISP

○ Use Static IP Address

    IP Address   0 . 0 . 0 . 0

    IP Subnet Mask   0 . 0 . 0 . 0

    Gateway IP Address   0 . 0 . 0 . 0

Domain Name Server (DNS) Address

⊙ Get Automatically From ISP

○ Use These DNS Servers

    Primary DNS   . . .

    Secondary DNS   . . .

Gateway's MAC Address

⊙ Use Default Address

○ Use This Computer's MAC Address

○ Use This MAC Address   00c002da8248

[Apply] [Cancel] [Test]

Figure 2-11: Browser-based configuration Basic Settings menu

Procedure 2-8: Manual Configuration

You can manually configure the gateway in the Basic Settings menu shown in Figure 2-11 using these steps:

1. If your ISP ADSL service requires setting the Multiplexing Method and VPI/VCI parameters, click on the ADSL Settings link from the main menu, fill in the settings your ISP provided, and click Apply. Usually the default settings will work fine and you can skip this step.

2. Click the Basic Settings link on the Setup menu. If your Internet connection does not require a login, fill in the settings according to the instructions below. If your Internet connection does require a login, click Yes, and skip to step 3.

    Select Yes if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.

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

    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. These fields are case sensitive.

    b. If you wish to change the login timeout, enter a new value in minutes. This determines how long the gateway keeps the Internet connection active after there is no Internet activity from the LAN. Entering an Idle Timeout value of zero means never log out.

    c. Domain Name Server (DNS) Address:
        If you know that your ISP does not automatically transmit DNS addresses to the gateway 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

3. If your Internet connection does require a login, click Yes at the top of the Basic Settings menu and fill in the settings according to the instructions below.

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

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

c. Domain Name Server (DNS) Address:
   If you know that your ISP does not automatically transmit DNS addresses to the gateway
   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.

   A DNS server is a host on the Internet that translates Internet names (such as
   www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of
   one or two DNS servers to your gateway during login. If the ISP does not transfer an
   address, you must obtain it from the ISP and enter it manually here. If you enter an address
   here, you should reboot your PCs after configuring the gateway.

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

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

4. Click Apply to save your settings.

5. Click on the Test button to test your Internet connection.
   If the NETGEAR website does not appear within one minute, refer to Chapter 7,
   "Troubleshooting".

Chapter 3
Wireless Configuration

This chapter describes how to configure the wireless features of your DG824M Wireless ADSL Modem Gateway.

Considerations For A Wireless Network

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your gateway in order to maximize the network speed. For further information on wireless networking, refer to "Wireless Networking" in Appendix B, "Network and Routing Basics."

Implement Appropriate Security

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. As a minimum precaution, change the SSID setting of all devices on your network from the factory setting to a unique password. Restricting access by MAC address filtering adds another obstacle against unwanted hosts joining your network. To hinder a determined eavesdropper, you should enable Wired Equivalent Privacy (WEP) data encryption. However, there may be a significant degradation of the data throughput on the wireless link when WEP is enabled.

Observe Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless gateway.

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

For best results, place your gateway:

- 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 2.4 GHz cordless phones.
- Away from large metal surfaces.

Wireless Settings

To configure the Wireless interface of your gateway, click the Wireless link in the main menu of the browser interface. The Wireless Settings menu will appear, as shown below:

Figure 3-1: Wireless Settings menu

In the Wireless Network section are the following parameters:

- **Identification**.

  — Regulatory Domain. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the gateway in a region other than the region shown here.

  — Station Name. The gateway model number.

  — SSID (Service Set ID). This is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. The same SSID must be assigned to all wireless devices in your network. The default SSID is **Wireless**.

- **Options.**

  — Channel No. 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.

  — WEP Status. Identifies the WEP options configured.

- **Access Point.**

  — All wireless stations. Any wireless station can connect.

  — Trusted PCs only. Only PCs with MAC address which you have specified can connect.

Procedure 3-1: Configuring Basic Wireless Network Settings

1. Choose an SSID for the gateway and all wireless PCs

   Devices on an 802.11b wireless network all share the same network name, or Service Set Identificatier (SSID). The first step in configuring your wireless network is to choose a secure value for your wireless network's SSID. In the SSID box, enter a value of up to 32 alphanumeric characters. This same SSID must be entered in the configuration of all PCs and devices connecting to this wireless network. The default SSID is Wireless.

   → **Note:** The SSID of any wireless access adapters must match the SSID you configure in the DG824M Wireless ADSL Modem Gateway. If they do not match, you will not get a wireless connection to the DG824M.

2. Set the Region of operation.

   Select the geopgraphic region in which the wireless interface will operate. This setting determines what radio frequencies will be available. It may not be legal to operate the gateway in a region other than the region shown here.

3. Set the Channel.

   This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your gateway. The default channel is 6.

4. For initial configuration and test, make sure that the Wireless Card Access List is set to Everyone and that Encryption Strength is set to Disabled.

   Note: These settings are not recommended for normal operation, but should be set initially to test basic wireless connectivity.

5. Click Apply to save your changes.

> → **Note:** If you are configuring the gateway from a wireless PC and you change the gateway's SSID, channel, or WEP settings, you will lose your wireless connection when you click on Apply. You must then change the wireless settings of your PC to match the gateway's new settings.

6. Configure and test your PCs for wireless connectivity.

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

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

Using the Wireless Access by MAC Address Feature

By default, any wireless PC that is configured with the correct SSID will be allowed access to your network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses. You can allow access by:

The Trusted PCs window displays a list of MAC addresses that will be allowed to connect to the gateway. These PCs must also be configured with SSID and WEP settings which match those of the DG824M.

Procedure 3-2: Restricting Wireless Access by MAC Address

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

1. From the Wireless Settings menu, click the Trusted PCs button to display the Wireless Access menu, shown below:

Wireless Access

Trusted PCs

11:22:33:44:55:66

Delete

Add new Trusted PC

Wireless Adapter Address

Add

Back

Figure 3-2.   Wireless Access menu

2. Click the Add button.

3. Enter the MAC address of the authorized PC. The MAC address is usually printed on the wireless card, or it may appear in the gateway's DHCP table.

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

> **Note:** If you are configuring the gateway from a wireless PC whose MAC address is not in the Trusted PC list, and you select Trusted PCs only, you will lose your wireless connection when you click on Apply. You must then access the gateway from a wired PC to make any further changes.

4. Click Add to save your entry.

5. Return to the Wireless Settings menu, select Trusted PCs only, then click Apply.

To delete a MAC address from the table, click on it to select it, then click the Delete button.

To edit a MAC address from the table, click on it to select it, then click the Edit or Delete button.

Configuring Wired Equivalent Privacy (WEP)

Wireless WEP

Authentication Type | Automatic
Automatic
Open System
Shared Key

Encryption
ryption
○ 64 Bit Encryption
○ 128 Bit Encryption

[Back] [Apply] [Cancel]
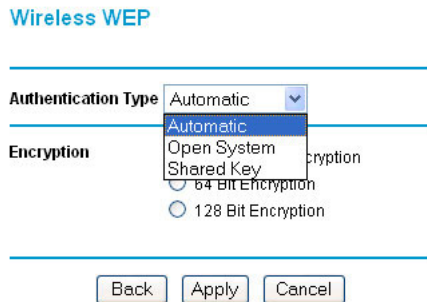
Figure 3-3.   Wireless WEP menu

In the Wireless Settings menu you can configure WEP data encryption using the following parameters:

• 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.

• Encryption Strength

The previous settings have determined which PCs will be allowed to access your wireless network, but have not added any protection from eavesdropping. With this setting, you can choose to have your data encrypted between the PCs and the gateway. Your choices are:

— Disable

No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.

— 64 or 128 bit WEP

Wireless Equivalent Privacy encryption will be applied. WEP provides some degree of privacy, but can be defeated without great difficulty.

— Keys

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

- Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate button. The keys will be automatically populated with key values. For 64-bit encryption, all four keys are generated from a single passphrase. With 128-bit encryption, each key can be generated with a different pasphrase.
- Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F) Select which of the four keys will be active.

Be sure to click Apply to save your settings in this menu.

Configuring WEP (Wired Equivalent Privacy)

If you have chosen to use WEP instead of IPSec, go to the Wireless Settings menu, click the Encryption Strength box and select either 64 Bit WEP or 128 Bit WEP. The Wireless Settings menu will display WEP setting fields, as shown below.

Figure 3-4.   Wireless Settings menu, WEP selected

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

- Manual - Enter 10 hexadecimal digits if 64 Bit WEP or 26 digits for 128 Bit WEP. Hexadecimal digits are 0-9, a-f, or A-F.

Wireless Configuration   3-7

- Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate button.

Select which of the four keys will be active.

Click Apply to save any settings from this menu.

Chapter 4
Protecting Your Network

This chapter describes how to use the basic firewall features of the DG824M Wireless ADSL Modem Gateway to protect your network.

Protecting Access to Your DG824M Wireless ADSL Modem Gateway

For security reasons, the gateway has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter **admin** for the gateway User Name and **password** for the gateway Password. You can use procedures below to change the gateway's password and the amount of time for the administrator's login timeout.

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

NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both upper and lower case letters, numbers, and symbols. Your password can be up to 30 characters.

Procedure 4-1: Changing the Built-In Password

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.

Figure 4-1: Log in to the gateway
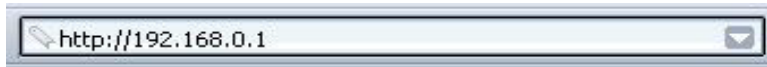
2. From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in Figure 4-2.

Figure 4-2: Set Password menu

3. To change the password, first enter the old password, and then enter the new password twice.

4. Click Apply to save your changes.

Note: After changing the password, you will be required to log in again to continue the configuration. If you have backed up the gateway settings previously, you should do a new backup so that the saved settings file includes the new password.

Procedure 4-1: Changing the Administrator Login Timeout

For security, the administrator's login to the gateway configuration will timeout after a period of inactivity. To change the login timeout period:

1. In the Set Password menu, type a number in 'Administrator login times out' field.The suggested default value is 5 minutes.

2. Click Apply to save your changes or click Cancel to keep the current period.

Configuring Basic Firewall Services

Basic firewall services you can configure include access blocking and scheduling of firewall security. These topics are presented below.

Blocking Keywords, Sites, and Services

The gateway provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the DG824M gateway prevents objectionable content from reaching your PCs. The Model RT311 router allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

• Blocks access from your LAN to Internet locations that you specify as off-limits.

• Keyword blocking of newsgroup names.

• Outbound Services Blocking limits access from your LAN to Internet locations or services that you specify as off-limits.

• Denial of Service (DoS) protection. Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.

• Blocks unwanted traffic from the Internet to your LAN.

The section below explains how to configure your gateway to perform these functions.

Procedure 4-2: Block Keywords and Sites

The DG824M gateway allows you to restrict access to Internet content based on functions such as Java or Cookies, Web addresses and Web address keywords.

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.

2.   Click on the Block Sites link of the Security menu.

Block Sites

☑ Turn keyword blocking on

[   ]
[Add Keyword]

Block sites containing these keywords or domain names:

[   ]

[Delete Keyword]   [Clear List]

Trusted IP Address   [0] . [0] . [0] . [0]

[Apply]   [Cancel]

Figure 4-3: Block Sites menu

3.   To enable keyword blocking, check "Turn keyword blocking on", enter a keyword or domain in the Keyword box, click Add Keyword, then click Apply.

Some examples of Keyword application follow:

- If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked, as is the newsgroup alt.pictures.xxx.

- If the keyword ".com" is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.

- Enter the keyword "." to block all Internet browsing access.

Up to 32 entries are supported in the Keyword list.

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

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

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

6. Click Apply to save your settings.

Rules

Firewall rules are used to block or allow specific traffic passing through from one side to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the DG824M are:

*   Inbound: Block all access from outside except responses to requests from the LAN side.

*   Outbound: Allow all access from the LAN side to the outside.

You may define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

To access the Rules configuration of the DG824M, click the Rules link on the main menu, then click Add for either an Outbound or Inbound Service.

Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
	Default	Yes	Any	ALLOW always	Any	Any	Never

Add   Edit   Move   Delete

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
	Default	Yes	Any	BLOCK always	--	Any	Match

Add   Edit   Move   Delete

☐ Default DMZ Server   192 . 168 . 0 . 0
☐ Respond to Ping on Internet WAN Port

Apply   Cancel

Figure 4-4: Rules menu

- To edit an existing rule, select its button on the left side of the table and click Edit.

- To delete an existing rule, select its button on the left side of the table and click Delete.

- To move an existing rule to a different position in the table, select its button on the left side of the table and click Move. At the script prompt, enter the number of the desired new position and click OK.

Inbound Rules (Port Forwarding)

Because the DG824M uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet. The rule tells the gateway to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

> **Note:** Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

Inbound Rule Example: A Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests from any outside IP address to the IP address of your web server at any time of day. This rule is shown in Figure 4-5:

Figure 4-5: Rule example: A Local Public Web Server

The parameters are:

- Service
  From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Add Services menu to add any additional services or applications that do not already appear.

- Action
  Choose how you would like this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.

- Send to LAN Server
  Enter the IP address of the PC or Server on your LAN which will receive the inbound traffic covered by this rule.

- WAN Users
  These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:

  - Any All IP addresses are covered by this rule.

  - Address range If this option is selected, you must enter the "Start" and "Finish" fields.

  - Single address Enter the required address in the "Start" fields.

- Log
  You can select whether the traffic will be logged. The choices are:

  - Never - no log entries will be made for this service.
  - Always - any traffic for this service type will be logged.
  - Match - traffic of this type which matches the parameters and action will be logged.
  - Not match - traffic of this type which does not match the parameters and action will be logged.

Inbound Rule Example: Allowing Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in Figure 4-6, CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.

Inbound Services

Service	CU-SEEME(TCP/UDP:7648)
Action	ALLOW always
Send to LAN Server	192 . 168 . 0 . 11
WAN Users	Address Range
	start: 134 . 177 . 88 . 1
	finish: 134 . 177 . 88 . 254
Log	Not Match

Back   Apply   Cancel

Figure 4-6: Rule example: Videoconference from Restricted Addresses

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menus so that external users can always find your network.

- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the PC's IP address constant.

- Local PCs must access the local server using the PCs' local LAN address (192.168.0.11 in the example in Figure 4-6 above). Attempts by local PCs to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The DG824M allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local PC based on:

- the IP address of the local PC (source address)
- the IP address of the Internet site being contacted (destination address)
- the time of day
- the type of service being requested (service port number)

Following is an application example of outbound rules:

Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the gateway log any attempt to use Instant Messenger during that blocked period.

Outbound Services

Service	AIM(TCP:5190)
Action	BLOCK by schedule,otherwise allow
LAN users	Any
	start: 0 . 0 . 0 . 0
	finish: 0 . 0 . 0 . 0
WAN Users	Any
	start: 0 . 0 . 0 . 0
	finish: 0 . 0 . 0 . 0
Log	Match

Back | Apply | Cancel

Figure 4-7: Rule example: Blocking Instant Messenger

The parameters are:

- Service
  From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Add Services menu to add any additional services or applications that do not already appear.

- Action
  Choose how you would like this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.

- LAN Users
  These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:

  - Any All IP addresses are covered by this rule.

  - Address range If this option is selected, you must enter the "Start" and "Finish" fields.

  - Single address Enter the required address in the "Start" fields.

- WAN Users
  These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the desired option:

  - Any All IP addresses are covered by this rule.

  - Address range If this option is selected, you must enter the "Start" and "Finish" fields.

  - Single address Enter the required address in the "Start" fields.

- Log
  You can select whether the traffic will be logged. The choices are:

  - Never - no log entries will be made for this service.
  - Always - any traffic for this service type will be logged.
  - Match - traffic of this type which matches the parameters and action will be logged.
  - Not match - traffic of this type which does not match the parameters and action will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in Figure 4-8:

Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
○	1	☑	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never

Add Edit Move Delete

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
⊙	1	☑	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
○	2	☑	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match

Add Edit Move Delete

☐ Default DMZ Server   192 . 168 . 0 . 0

☐ Respond to Ping on Internet WAN Port

Apply Cancel

Figure 4-8: Rules table with examples

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

Services

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 the Internet sends a request for service to a server computer, 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.

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.

Although the DG824M already holds a list of many service port numbers, you are not limited to these choices. Use the procedure below to create your own service definitions.

Procedure 4-3: Define Services

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.

2. Click on the Services link of the Security menu to display the Services menu shown in Figure 4-9:

Services

Service Table

	#	Name	Type	Ports (TCP or UDP)

[Add Custom Service] [Edit Service] [Delete Service]

Figure 4-9: Services menu

- To create a new Service, click the Add button.

- To edit an existing Service, select its button on the left side of the table and click Edit.

- To delete an existing Service, select its button on the left side of the table and click Delete.

3. Modify the menu shown below for defining or editing a service.

Figure 4-10: Add Services menu

4. Click Apply to save your changes.

Setting Times and Scheduling Firewall Services

The DG824M gateway 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 select your Time Zone from the list.

Procedure 4-4: Setting Your Time Zone

In order to localize the time for your log entries, you must specify your Time Zone:

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.

2. Click on the Schedule link of the Security menu to display menu shown below.

Figure 4-11: Schedule Services menu

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

   Check the Daylight Savings Time box if your time zone is currently in daylight savings time.

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

4. The gateway has a list of publicly available NTP servers. If you would prefer to use a particular NTP server as the primary server, enter its IP address under Use this NTP Server.

5. Click Apply to save your settings.

Procedure 4-5: Scheduling Firewall Services

If you enabled services blocking in the Block Services menu or Port forwarding in the Ports menu, you can set up a schedule for when blocking occurs or when access isn't restricted.

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.

2. Click on the Schedule link of the Security menu to display menu shown above in the Schedule Services menu.

3. To block Internet services based on a schedule, select Every Day or select one or more days. If you want to limit access completely for the selected days, select All Day. Otherwise, to limit access during certain times for the selected days, enter Start Blocking and End Blocking times.

   Note: Enter the values as 24-hour time. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes.

4. Click Apply to save your changes.

Chapter 5
Managing Your Network

This chapter describes how to perform network management tasks with your DG824M Wireless ADSL Modem Gateway.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the DG824M gateway are stored in a configuration file in the gateway. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.

Procedure 5-6: Backup the Configuration to a File

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the gateway.

2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in Figure 5-1.

Settings Backup

Save a copy of current settings

    Back Up

Restore saved settings from file

    [   ]   Browse...

    Restore

Revert to factory default settings

    Erase

Figure 5-1: Settings Backup menu

3. Click Backup to save a copy of the current settings.

4. Store the `.cfg` file on a computer on your network.

Procedure 5-7: Restore a Configuration from a File

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the gateway.

2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in Figure 5-1.

3. Enter the full path to the file on your network or click the Browse button to browse to the file.

4. When you have located the .cfg file, click the Restore button to upload the file to the gateway.

5. The gateway will then reboot automatically.

Procedure 5-8: Erase the Configuration

It is sometimes desirable to restore the gateway to the factory default settings. This can be done by using the Erase function.

1. To erase the configuration, from the Maintenance menu Settings Backup link, click the Erase button on the screen.

2. The gateway will then reboot automatically.

   After an erase, the gateway's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

Note: To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the gateway. See "DG824M Rear Panel" on page 1-8.

Upgrading the Gateway's Firmware

The software of the DG824M gateway is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

Upgrade files can be downloaded from NETGEAR's website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN or .IMG) file before uploading it to the gateway.

Procedure 5-1: Gateway Upgrade

Note: NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you may need to restore your configuration settings.

1. Download and unzip the new software file from NETGEAR.

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

2. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the gateway.

3. From the Main Menu of the browser interface, under the Maintenance heading, select the Gateway Upgrade heading to display the menu shown in Figure 5-2.

Figure 5-2: Gateway Upgrade menu

4. In the Gateway Upgrade menu, click the **Browse** to locate the binary (.BIN or .IMG) upgrade file.

5. Click **Upload**.

Note: When uploading software to the gateway, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your gateway will automatically restart. The upgrade process will typically take about one minute. In some cases, you may need to clear the configuration and reconfigure the gateway after upgrading.

Network Management Information

The DG824M provides a variety of status and usage information which is discussed below.

Viewing Gateway Status and Usage Statistics

From the Main Menu, under Maintenance, select Gateway Status to view the screen in Figure 5-3.

Gateway Status

System Name	DG824
Firmware Version	Version 1.0 Release 08
WAN Port	
MAC Address	00:C0:02:DA:82:48
IP Address	
DHCP	Client
IP Subnet Mask	0.0.0.0
Domain Name Server	
LAN Port	
MAC Address	00:C0:02:DA:82:47
IP Address	192.168.0.1
DHCP	Server
IP Subnet Mask	255.255.255.0
ADSL Modem	
ADSL Firmware Version	53050
Modem Status	Connecting
Connect Mode	LLC-BASED
Downstream Speed	0 Kbps
Upstream Speed	0 Kbps
VPI	8
VCI	35

[Show Statistics]   [Show WAN Status]

Figure 5-3: Gateway Status screen

The Router Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, under Maintenance, select Router Status to view the status screen, shown in Figure 5-3.

This screen shows the following parameters:

Table 5-1.   Menu 3.2 - Gateway Status Fields

Field	Description
System Name	The Host Name assigned to the gateway in the Basic Settings menu.
Firmware Version	This field displays the gateway firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the gateway.
MAC Address	This field displays the Ethernet MAC address being used by the Internet (WAN) port of the gateway.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the gateway. If no address is shown, the gateway cannot connect to the Internet.
DHCP	If None, the gateway will use a fixed IP address on the WAN. If Client, the gateway will obtain an IP address dynamically from the ISP
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the gateway.
Domain Name Servers (DNS)	This field displays the DNS Server IP addresses being used by the gateway. These addresses are usually obtained dynamically from the ISP.
LAN Port	These parameters apply to the Local (WAN) port of the gateway.
MAC Address	This field displays the Ethernet MAC address being used by the Local (LAN) port of the gateway.
IP Address	This field displays the IP address being used by the Local (LAN) port of the gateway. The default is 192.168.0.1
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the gateway. The default is 255.255.255.0
DHCP	If OFF, the gateway will not assign IP addresses to PCs on the LAN. If ON, the gateway will assign IP addresses to PCs on the LAN.
ADSL Modem	These parameters apply to the Local (WAN) port of the gateway.
ADSL Firmware Version	The version of the firmware.
Modem Status	The connection status of the modem.
Downstream Speed	The speed at which the modem is receiving data from the ADSL line.
Upstream Speed	The speed at which the modem is transmitting data to the ADSL line.
VPI	The VPI setting.
VCI	The VCI setting.

Click on the "Show Statistics" button to display gateway usage statistics, as shown in Figure 5-3 below:

System Up Time 3:10:5

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	10M/Half	6529	147307	0	118	0	3:10:5
LAN	100M/Full	8440	11540	0	673	404	3:10:5
Serial	Not Connected	0	0	n/a	0	0	0:0:0

Poll Interval : 5 (secs)   [Set Interval]   [Stop]

Figure 5-4: Gateway Statistics screen

This screen shows the following statistics:.

Table 5-1.   Gateway Statistics Fields

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

Click on the "Show WAN Status" button to display gateway WAN connection status, as shown in Figure 5-5 below:

Connection Time	02:03:53
Connection Method	Dynamic IP
IP Address	
Network Mask	0.0.0.0
Default Gateway	0.0.0.0

Renew

Figure 5-5: Gateway WAN Status screen

Clicking the Renew button updates the status information.

This screen shows the following statistics:.

Table 5-1.   Gateway Statistics Fields

Field	Description
Connection Time	The time elapsed since the last connection to the Internet via the ADSL port.
Connection Method	The method the ADSL port acquired its TCP/IP configuration.
IP Address	The IP Address assigned to the WAN port by the ADSL Internet Service Provider.
Network Mask	Then Network Mask assigned to the WAN port by the ADSL Internet Service Provider.
Default Gateway	Then Default Gateway router assigned to the WAN port by the ADSL Internet Service Provider.

Viewing Attached Devices

The Attached Devices menu contains a table of all IP devices that the gateway has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown in Figure 5-6

Attached Devices

#	IP Address	Device Name	MAC Address
1	192.168.0.2	emachine	00:48:54:8d:d7:d3

Refresh
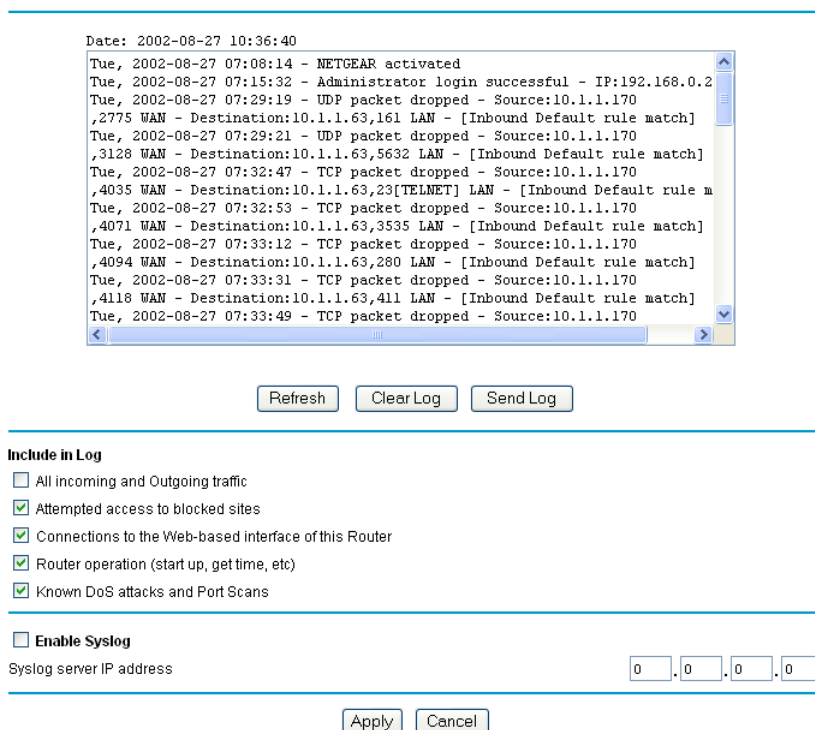
Figure 5-6: Attached Devices menu

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

Viewing, Selecting, and Saving Logged Information

The gateway will log security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites menu, the Logs page shows you when someone on your network tried to access a blocked site. If you enabled e-mail notification, you'll receive these logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs here. An example is shown below.

Logs

```
Date: 2002-08-27 10:36:40
Tue, 2002-08-27 07:08:14 - NETGEAR activated
Tue, 2002-08-27 07:15:32 - Administrator login successful - IP:192.168.0.2
Tue, 2002-08-27 07:29:19 - UDP packet dropped - Source:10.1.1.170
,2775 WAN - Destination:10.1.1.63,161 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:29:21 - UDP packet dropped - Source:10.1.1.170
,3128 WAN - Destination:10.1.1.63,5632 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:32:47 - TCP packet dropped - Source:10.1.1.170
,4035 WAN - Destination:10.1.1.63,23[TELNET] LAN - [Inbound Default rule m
Tue, 2002-08-27 07:32:53 - TCP packet dropped - Source:10.1.1.170
,4071 WAN - Destination:10.1.1.63,3535 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:12 - TCP packet dropped - Source:10.1.1.170
,4094 WAN - Destination:10.1.1.63,280 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:31 - TCP packet dropped - Source:10.1.1.170
,4118 WAN - Destination:10.1.1.63,411 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:49 - TCP packet dropped - Source:10.1.1.170
```

[Refresh]   [Clear Log]   [Send Log]

Include in Log
- ☐ All incoming and Outgoing traffic
- ☑ Attempted access to blocked sites
- ☑ Connections to the Web-based interface of this Router
- ☑ Router operation (start up, get time, etc)
- ☑ Known DoS attacks and Port Scans

☐ **Enable Syslog**
Syslog server IP address   [0] . [0] . [0] . [0]

[Apply]   [Cancel]

Figure 5-7: Security Logs menu

Log entries are described in Table 5-1

Table 5-1.   Security Log entry descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Description or Action	The type of event and what action was taken if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN
Destination	The name or IP address of the destination device or website.
Destination port and interface	The service port number of the destination device, and whether it's on the LAN or WAN.

Log action buttons are described in Table 5-8

Table 5-8:   Security Log action buttons

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to email the log immediately.
Apply	Click this button to apply the current settings.
Cancel	Click this button to clear the current settings.

Selecting What Information to Log

Besides the standard information listed above, you can choose to log additional information. Those optional selections are as follows:

- All incoming and outgoing traffic

- Attempted access to blocked site

- Connections to the Web-based interface of this Router

- Router operation (start up, get time, etc.)

- Known DoS attacks and Port Scans

Saving Log Files on a Server

You can choose to write the logs to a PC running a syslog program. To activate this feature, check the box under Syslog and enter the IP address of the server where the log file will be written.

Examples of log messages

Following are examples of log messages. In all cases, the log entry shows the timestamp as: Day, Year-Month-Date Hour:Minute:Second

Activation and Administration

```
Tue, 2002-05-21 18:48:39 - NETGEAR activated
```

[This entry indicates a power-up or reboot with initial time entry.]

```
Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2
Thu, 2002-05-21 18:56:58 - Administrator logout - IP:192.168.0.2
```

[This entry shows an administrator logging in and out from IP address 192.168.0.2.]

```
Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

[This entry shows a time-out of the administrator login.]

```
Wed, 2002-05-22 22:00:19 - Log emailed
```

[This entry shows when the log was emailed.]

Dropped Packets

```
Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

[These entries show an inbound FTP (port 21) packet, UDP packet (port 6970), and ICMP packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

Enabling Security Event E-mail Notification

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

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.

[Apply] [Cancel]

- Turn e-mail notification on
  Check this box if you wish to receive e-mail logs and alerts from the gateway.

- Your outgoing mail server
  Enter the name or IP address 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 a significant security event, such as a known attack, port scan, or 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 gateway's memory. If the gateway cannot e-mail the log file, the log buffer may fill up. In this case, the gateway overwrites the log and discards its contents.

Running Diagnostic Utilities and Rebooting the Router

The DG824M gateway has a diagnostics feature. You can use the diagnostics menu to perform the following functions from the gateway:

- Ping an IP Address to test connectivity to see if you can reach a remote host.

- Perform a DNS Lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.

- Display the Routing Table to identify what other routers the router is communicating with.

- Trace the Routing Path to identify any connectivity or congestion problems in the network.

- Reboot the Router to enable new network configurations to take effect or to clear problems with the router's network connection.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Diagnostics heading to display the menu shown in Figure 5-9.

Figure 5-9: Diagnostics menu

Enabling Remote Management

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your NETGEAR Cable/DSL ProSafe VPN Firewall.

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

Procedure 5-2: Configure Remote Management

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the gateway.

2. From the Advanced section of the main menu, click on the Remote Management link.

3. Select the Allow Remote Management check box.

4. Specify what external addresses will be allowed to access the gateway's remote management.

    For security, NETGEAR recommends that you restrict access to as few external IP addresses as practical.

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

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

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

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

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

6. Click Apply to have your changes take effect.

    When accessing your gateway from the Internet, you will type your gateway's WAN IP address in your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter in your browser:

    ```
    http://134.177.0.123:8080
    ```

    Note: In this case, the http:// must be included in the address.

This chapter describes how to configure the advanced features of your DG824M Wireless ADSL Modem Gateway.

Configuring Advanced Security

The DG824M Wireless ADSL Modem Gateway provides a variety of advanced features, such as:

*   Setting up a Demilitarized Zone (DMZ) Server

*   The flexibility of configuring your LAN TCP/IP settings

These features are discussed below.

Setting Up A Default DMZ Server

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

> **Note:** For security, you should avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

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

Procedure 6-1: Configuring A Default DMZ Server.

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

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the gateway.

2. From the Main Menu, under Security, click the Rules link to view the menu, shown in Figure 6-1

Figure 6-1: Security Rules Menu

3. Click Default DMZ Server.

4. Type the IP address for that server.

5. Click Apply to save your changes.

Respond to Ping on Internet WAN Port

If you want the gateway 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 gateway to be discovered. Don't check this box unless you have a specific reason to do so.

Configuring LAN IP Settings

The LAN IP Setup menu allows configuration of LAN IP services such as DHCP and RIP. These features can be found under the Advanced heading in the Main Menu of the browser interface.

LAN TCP/IP Setup

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

•   LAN IP addresses—192.168.0.1

•   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.

LAN IP Setup

LAN TCP/IP Setup

IP Address	192 . 168 . 0 . 1	
IP Subnet Mask	255 . 255 . 255 . 0	
RIP Direction	None	
RIP Version	Disabled	

MTU Size

⊙ Default (1500)   ○ Custom 1500

☑ **Use router as DHCP server**

Starting IP Address	192 . 168 . 0 . 2	
Ending IP Address	192 . 168 . 0 . 51	

Reserved IP Table

#	IP Address	Mac Address	Device Name

Add   Edit   Delete

Apply   Cancel

Figure 6-2: LAN IP Setup Menu

The LAN TCP/IP Setup parameters are:

• IP Address
This is the LAN IP address of the gateway.

• IP Subnet Mask
This is the LAN Subnet Mask of the gateway. 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 gateway sends and receives RIP packets. Both is the default.

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

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

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

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

— RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.

— RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.

— RIP-2B uses subnet broadcasting.

— RIP-2M uses multicasting.

→ **Note:** If you change the LAN IP address of the gateway 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.

MTU Size

The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For PPPoE, the gateway adjusts the MTU size automatically. Changing this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

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

1. Under MTU Size, select Custom.

2. Enter a new size between 64 and 1500. For PPPoE, use 1492.

3. Click Apply to save the new configuration.

DHCP

By default, the gateway 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 gateway. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the gateway 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.

Use Gateway as DHCP server

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 gateway's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.253, although you may wish to save part of the range for devices with fixed addresses.

The gateway 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 is the gateway's LAN IP address

• Primary DNS Server, if you entered a Primary DNS address in the Basic Settings menu; otherwise, the gateway's LAN IP address

• Secondary DNS Server, if you entered a Secondary DNS address in the Basic Settings menu

- WINS Server, short for *Windows Internet Naming Service Server,* determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

Reserved IP addresses

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

To reserve an IP address:

1. Click the **Add** button.

2. In the IP Address box, type the IP address to assign to the PC or server.
   Choose an IP address from the router's LAN subnet, such as 192.168.0.X.

3. Type the MAC Address of the PC or server.
   Tip: If the PC is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.

4. Click **Apply** to enter the reserved address into the table.

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

To edit or delete a reserved address entry:

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

2. Click Edit or Delete.

Procedure 6-1: Configure LAN TCP/IP Setup

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the gateway.

2. From the Main Menu, under Advanced, click the LAN IP Setup link to view the menu, shown in Figure 6-3

LAN IP Setup

LAN TCP/IP Setup

IP Address	192 . 168 . 0 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	None
RIP Version	Disabled

MTU Size

    ⦿ Default (1500)   ○ Custom 1500

☑ **Use router as DHCP server**

Starting IP Address	192 . 168 . 0 . 2
Ending IP Address	192 . 168 . 0 . 51

Reserved IP Table

#	IP Address	Mac Address	Device Name

[Add] [Edit] [Delete]

[Apply] [Cancel]

Figure 6-3: LAN IP Setup Menu

3. Enter the TCP/IP, MTU, DHCP, or Reserved IP parameters.

4. Click Apply to save your changes.

Configuring Dynamic DNS

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

The gateway contains a client that can connect to a dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the gateway, whenever your ISP-assigned IP address changes, your gateway will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

Procedure 6-2: Configure Dynamic DNS

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the gateway.

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

3. Access the website of one of the dynamic DNS service providers whose names appear in the 'Select Service Provider' box, and register for an account.
   For example, for dyndns.org, go to www.dyndns.org.

4. Select the "Use a dynamic DNS service" check box.

5. Select the name of your dynamic DNS Service Provider.

6. Type the Host Name that your dynamic DNS service provider gave you.
   The dynamic DNS service provider may call this the domain name. If your URL is myName.dyndns.org, then your Host Name is "myName."

7. Type the User Name for your dynamic DNS account.

8. Type the Password (or key) for your dynamic DNS account.

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

10. Click Apply to save your configuration.

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

Using Static Routes

Static Routes provide additional routing information to your gateway. Under normal circumstances, the gateway 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.

Static Route Example

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

- Your primary Internet access is through a cable modem to an ISP.

- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.

- Your company's network is 134.177.0.0.

When you first configured your gateway, 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 gateway will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your gateway that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like Figure 6-5.

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.
  This represents the number of routers between your network and the destination. This is a direct connection so it is set to 1.

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

Procedure 6-3: Configuring Static Routes

1. Log in to the gateway at its default LAN address of http://192.168.0.1 with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the gateway.

2. From the Main Menu of the browser interface, under Advanced, click on Static Routes to view the Static Routes menu, shown in Figure 6-4.

Static Routes

	#	Active	Name	Destination	Gateway
◉	1	YES	isdn_rtr	134.177.0.0	192.168.0.100

Add   Edit   Delete

Figure 6-4: Static Routes Table

3. To add or edit a Static Route:

   a. Click the **Edit** button to open the Edit Menu, shown in Figure 6-5.

   Static Routes

Route Name	isdn_rtr
☑ Private	
☑ Active	
Destination IP Address	134 . 177 . 0 . 0
IP Subnet Mask	255 . 255 . 0 . 0
Gateway IP Address	192 . 168 . 0 . 100
Metric	1

   Apply   Cancel

Figure 6-5: Static Route Entry and Edit Menu

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

c. Select **Active** to make this route effective.

d. Select **Private** if you want to limit access to the LAN only.
   The static route will not be reported in RIP.

e. Type the Destination IP Address of the final destination.

f. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type 255.255.255.255.

g. Type the Gateway IP Address, which must be a router on the same LAN segment as the gateway.

h. 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.

4. Click **Apply** to have the static route entered into the table.

Chapter 7
Troubleshooting

This chapter gives information about troubleshooting your DG824M Wireless ADSL Modem Gateway. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the gateway on?

- Have I connected the gateway correctly?

- I can't access the gateway's configuration with my browser.

- I've configured the gateway but I can't access the Internet.

- I can't remember the gateway's configuration password.

- I want to clear the configuration and start over again.

Basic Functioning

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

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

2. Verify that the Test LED ✓ lights within a few seconds, indicating that the self-test procedure is running.

3. After approximately 10 seconds, verify that:

    a. The Test LED is not lit.

    b.   The LAN port LEDs are lit for any local ports that are connected.

    c.   The WAN port LED is lit.

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

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

Power LED Not On

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

*   Make sure that the power cord is properly connected to your gateway and that the power supply adapter is properly connected to a functioning power outlet.

*   Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

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

Test LED Never Turns On or Test LED Stays On

When the gateway is turned on, the Test LED turns on for about 10 seconds and then turns off. If the Test LED does not turn on, or if it stays on, there is a fault within the gateway.

If you experience problems with the Test LED:

*   Cycle the power to see if the gateway recovers and the LED blinks for the correct amount of time.

If all LEDs including the Test LED are still on one minute after power up:

*   Cycle the power to see if the gateway recovers.

*   Clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. This procedure is explained in "Using the Default Reset button" on page 7-9.

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

LAN or WAN Port LEDs Not On

If either the LAN LEDs or WAN LED do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the gateway 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 gateway's WAN ADSL port, use the cable that was supplied with the DG824M.

Troubleshooting the Web Configuration Interface

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

- If you are using an Ethernet-connected PC, check the Ethernet connection between the PC and the gateway as described in the previous section.

- Make sure your PC's IP address is on the same subnet as the gateway. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to "Verifying TCP/IP Properties" on page C-6 or "Verifying TCP/IP Properties for Macintosh Computers" on page C-17 to find your PC's IP address. Follow the instructions in Appendix C to configure your PC.

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

- If your gateway's IP address has been changed and you don't know the current IP address, clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. This procedure is explained in "Using the Default Reset button" on page 7-9.

- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.

- Try quitting the browser and launching it again.

- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the gateway 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 gateway is unable to access the Internet, you should check the ADSL connection, then the WAN TCP/IP connection.

ADSL link

If your gateway is unable to access the Internet, you should first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the WAN LED.

WAN LED Green or Blinking Green

If your WAN LED is green or blinking green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

WAN LED Blinking Yellow

If your WAN LED is blinking yellow then your gateway is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the WAN LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green WAN LED there may be a problem with your wiring. If the telephone company has tested the ADSL signal at your Network Interface Device (NID), then you may have poor quality wiring in your house.

WAN LED Off

If the WAN LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being careful to use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green WAN LED the problem may be one of the following:

- Check that the telephone company has made the connection to your line and tested it.

- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It may be necessary to use a swapper if you ADSL signal is on pins 1 and 4 or the RJ-11 jack. The DG824M gateway uses pins 2 and 3.

Obtaining a WAN IP Address

If your gateway is unable to access the internet, and your WAN LED is green or blinking green, you should determine whether the gateway is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your gateway must request an IP address from the ISP. You can determine whether the request was successful using the browser interface.

To check the WAN IP address from the browser interface:

1. Launch your browser and select an external site such as www.netgear.com

2. Access the Main Menu of the gateway's configuration at http://192.168.0.1

3. Under the Maintenance heading check that an IP address is shown for the WAN Port
   If 0.0.0.0 is shown, your gateway has not obtained an IP address from your ISP.

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

- Your ISP may require a Multiplexing Method or VPI/VCI parameter.
  Verify with your ISP the Multiplexing Method and parameter value, and update the gateway's Basic Settings accordingly.

- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or PPP over ATM (PPPOA) login.

- If you have selected a login program, you may have incorrectly set the Service Name, User Name and Password. See "Troubleshooting PPPoE or PPPoA", below.

- Your ISP may check for your PC's host name.
  Assign the PC Host Name of your ISP account to the gateway in the browser-based Setup Wizard.

- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your PC's MAC address. In this case:

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

  OR

  Configure your gateway to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to "Manually Configuring Your Internet Connection" on page 2-17.

Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

1. Access the Main Menu of the gateways configuration at http://192.168.0.1.

2. Under the Maintenance heading, click the "Show WAN Status" button.

3. If all of the steps indicate "OK" then your PPPoE or PPPoA connection is up and working.

4. If any of the steps indicates "Failed", you can attempt to reconnect by clicking "Connect". The gateway will continue to attempt to connect indefinitely.

If you cannot connect after several minutes, you may be using an incorrect Service Name, User Name or Password. There also may be a provisioning problem with your ISP.

> **Note:** Unless you connect manually, the gateway will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshooting Internet Browsing

If your gateway can obtain an IP address but your PC is unable to load any web pages from the Internet:

- Your PC may not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the gateway's configuration, reboot your PC and verify the DNS address as described in "Verifying TCP/IP Properties" on page C-6. Alternatively, you may configure your PC manually with DNS addresses, as explained in your operating system documentation.

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

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

Troubleshooting a TCP/IP Network Using the Ping Utility

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

Testing the LAN Path to Your Router

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

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

1. From the Windows toolbar, click on the Start button and select Run.

2. In the field provided, type Ping followed by the IP address of the router, as in this example:

   ping 192.168.0.1

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

Troubleshooting   7-7

— Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or WAN Port LEDs Not On" on page 7-2.

— Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.

• Wrong network configuration

— Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.

— Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

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

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

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

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

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

— Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

— Check that your cable or DSL modem is connected and functioning.

— If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to "clone" or "spoof" the MAC address from the authorized PC. Refer to "Manually Configuring Your Internet Connection" on page 2-17.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the Web Configuration Manager (see "Backing Up, Restoring, or Erasing Your Settings" on page 5-1).

- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

Using the Default Reset button

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

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).

2. Release the Default Reset button and wait for the router to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The DG824M gateway uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

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

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

Appendix A
Technical Specifications

This appendix provides technical specifications for the DG824M Wireless ADSL Modem Gateway.

Network Protocol and Standards Compatibility

Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP, PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA), RFC 1483 Bridged Ethernet

Power Adapter

North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	15 V AC @ 1.0A output, 30W maximum

Physical Specifications

Dimensions:	10" x 6.7" x 1.3" 255 mm x 169 mm x 34 mm
Weight:	1.4 lbs. 0.62 kg

Environmental Specifications

Operating temperature:	0° to 40° C (32° to 104° F)

Operating humidity:	90% maximum relative humidity, noncondensing

Electromagnetic Emissions

Meets requirements of:	FCC Part 15 Class B
	VCCI Class B
	EN 55 022 (CISPR 22), Class B

Interface Specifications

LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	ADSL, Dual RJ-11, pins 2 and 3
	T1.413, G.DMT, G.Lite
	ITU Annex B

Appendix B
Network and Routing Basics

This chapter provides an overview of IP networks, routing, and wireless 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 DG824M Wireless ADSL Modem Gateway 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 DG824M gateway 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.

Class A

Network   Node

Class B

            Network   Node

Class C
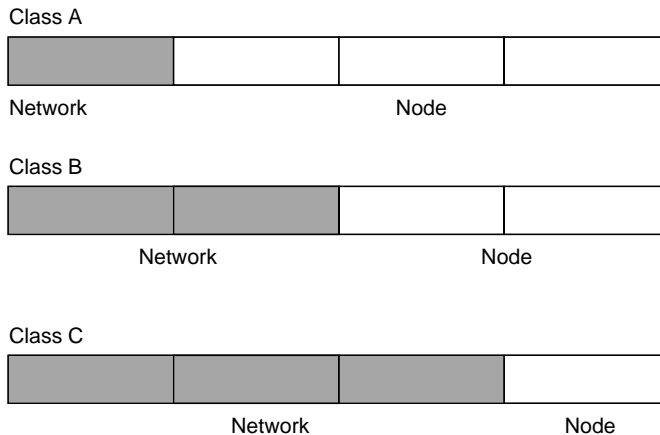
            Network   Node

Figure 7-1: 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.`

Network and Routing Basics   B-3

- 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.

Class B

Figure 7-2: 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 7-1.   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 7-2.   Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16

Table 7-2.   Netmask Formats

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

NETGEAR strongly recommends that you 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
```

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the DG824M gateway 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 PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The DG824M gateway employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

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

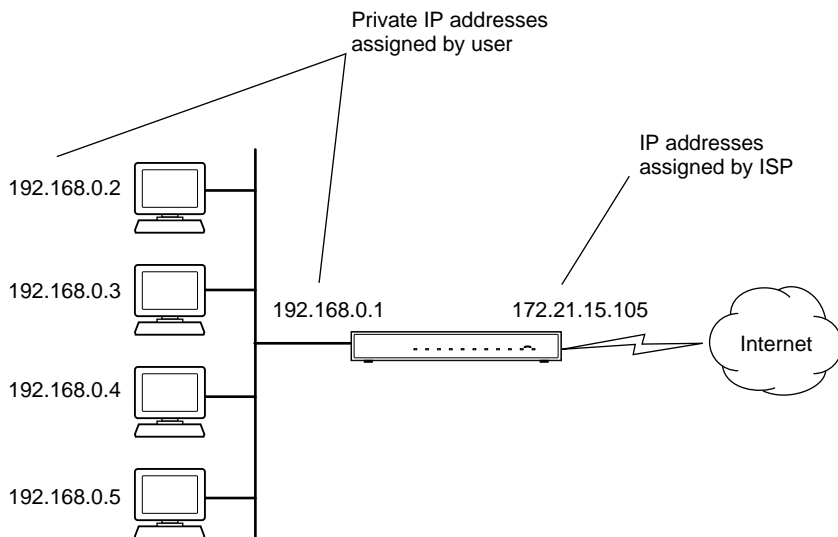The following figure illustrates a single IP address operation.

Figure 7-3: Single IP Address Operation Using NAT

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

MAC Addresses and Address Resolution Protocol

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

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

Related Documents

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

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

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

Domain Name Server

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

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

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The DG824M gateway has the capacity to act as a DHCP server.

The DG824M gateway also functions as a DHCP client when connecting to the ISP. The gateway can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

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 in Table 7-1.

Table 7-1.   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	

Uplink Switches and Crossover Cables

In the wiring table, the concept of transmit and receive are from the perspective of the PC. For example, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

Cable Quality

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.

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 Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

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

Stateful Packet Inspection

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

Denial of Service Attack

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

Wireless Networking

The DG824M gateway conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard for wireless LANs (WLANs). On an 802.11b wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected.

The 802.11b 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 802.11b devices.

Wireless Network Configuration

The 802.11b standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

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.

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.

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 Extended Service Set Identification (ESSID) is used, but may still be referred to as SSID.

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

Authentication and WEP 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 two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

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

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.

Wireless Channel Selection

IEEE 802.11 wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4Ghz and 2.5Ghz. Neighboring channels are 5Mhz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum12.5Mhz 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 are listed in Table 7-2:

Table 7-2.   802.11 Radio Frequency Channels

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

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

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

Appendix C
Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the Model RP614 Web Safe Router and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

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

Preparing Your Computers for TCP/IP Networking

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

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

- Windows® 95 or later includes the software components for establishing a TCP/IP network.

- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/ IP application package such as NetManage Chameleon.

- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.

• All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

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

The RP614 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—192.168.0.2 through 192.168.0.254

• Subnet mask—255.255.255.0

• Gateway address (the firewall)—192.168.0.1

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

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

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

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

2. Double-click the Network icon.

   The Network window opens, which displays a list of installed components:
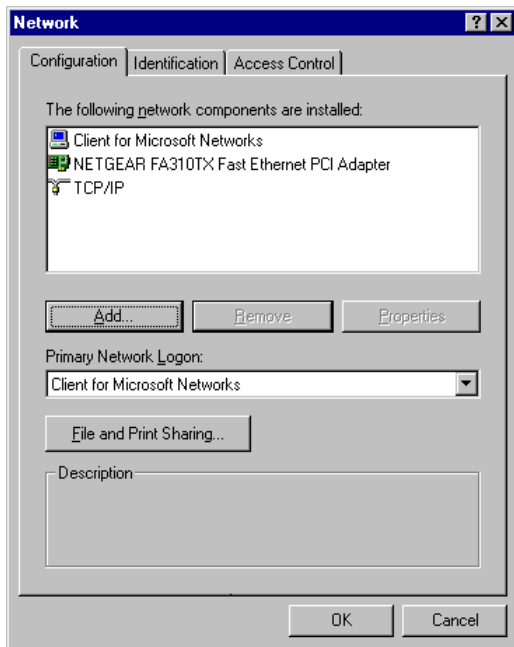
You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

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

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

a.   Click the Add button.

b.   Select Adapter, and then click Add.

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

If you need TCP/IP:

a.   Click the Add button.

b.   Select Protocol, and then click Add.

c.   Select Microsoft.

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

If you need Client for Microsoft Networks:

a. Click the Add button.

b. Select Client, and then click Add.

c. Select Microsoft.

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

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

Enabling DHCP to Automatically Configure TCP/IP Settings 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.

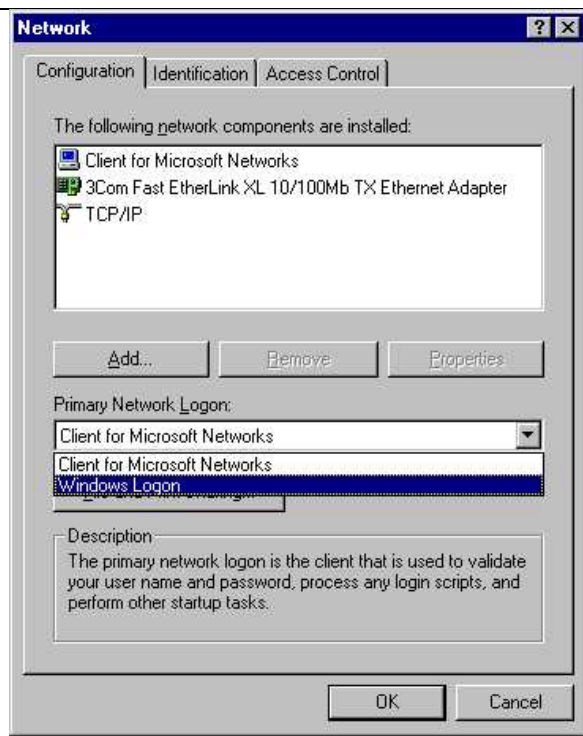**1**

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

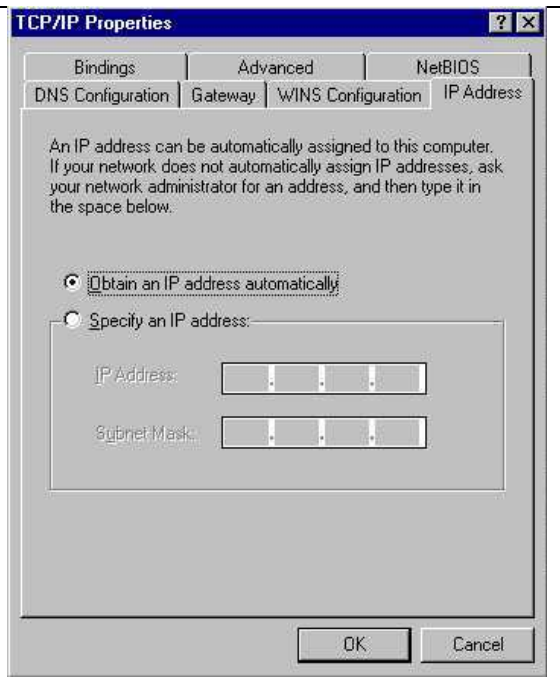Click on the **Properties** button. The following TCP/IP Properties window will display.

Network ? ☒

Configuration | Identification | Access Control |

The following network components are installed:

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

Add... | Remove | Properties

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.

OK | Cancel

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                                    ? X

  Bindings      |      Advanced      |      NetBIOS
DNS Configuration | Gateway | WINS Configuration | IP Address

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:     [   .   .   .   ]


                              OK          Cancel
```

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 192.168.0.2 and 192.168.0.254

   • The subnet mask is 255.255.255.0

   • The default gateway is 192.168.0.1

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**.
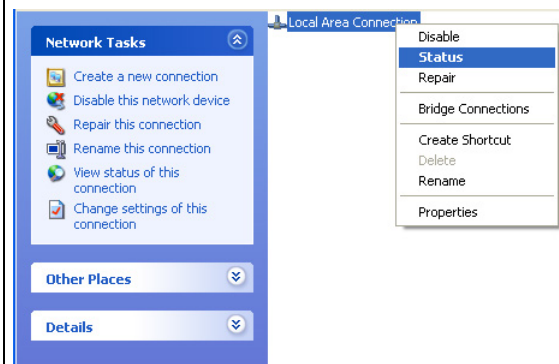
3

- 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

[Properties] [Disable]

[Close]
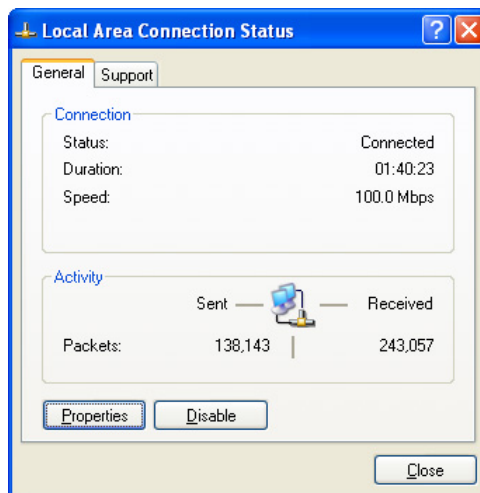
4

- 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

[Configure...]

This connection uses the following items:
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

[Install...] [Uninstall] [Properties]

Description
Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

[OK] [Cancel]

5

- Verify that the **Obtain an IP address automatically** radio button is selected.

- Verify that **Obtain DNS server address automatically** radio button is selected.

- Click the **OK** button.

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

Repeat these steps for each PC with this version of Windows on your network.
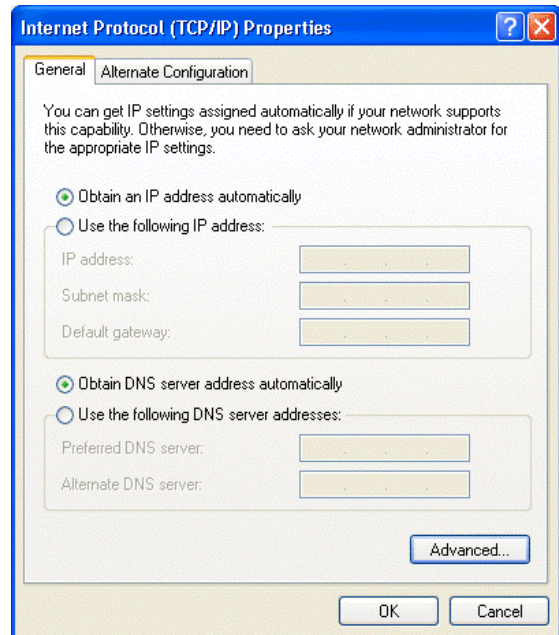
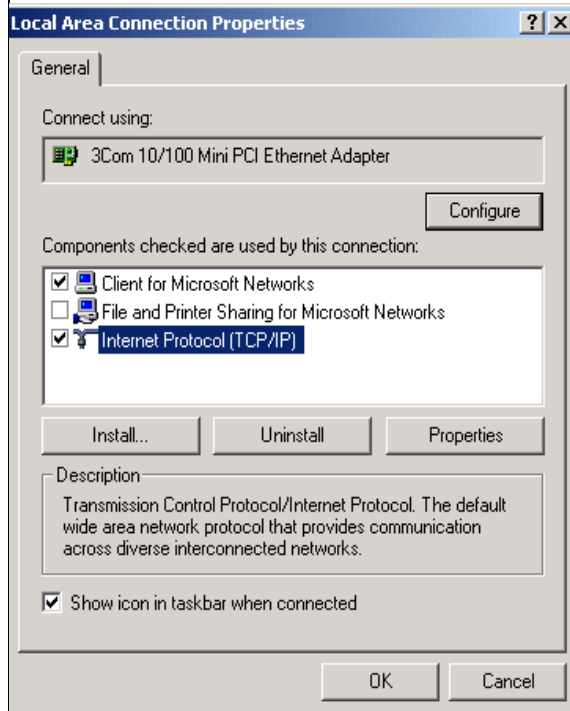## DHCP Configuration of TCP/IP in Windows 2000

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

1

- Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.

- Right click on **Local Area Connection** and select **Properties**.

2

- The **Local Area Connection Properties** dialog box appears.

- Verify that you have the correct Ethernet card selected in the **Connect using:** box.

- Verify that at least the following two items are displayed and selected in the box of "Components checked are used by this connection:"

  - Client for Microsoft Networks and

  - Internet Protocol (TCP/IP)

- Click **OK**.

Local Area Connection Properties ?|X|

General

Connect using:

  3Com 10/100 Mini PCI Ethernet Adapter

Configure

Components checked are used by this connection:

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

Install... | Uninstall | Properties

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

OK | Cancel

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 ? X

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:

  Advanced...

  OK   Cancel

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 ? X

General

Connect using:

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

Configure

Components checked are used by this connection:

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

Install...   Uninstall   Properties

Description

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

☐ Show icon in taskbar when connected

OK   Cancel
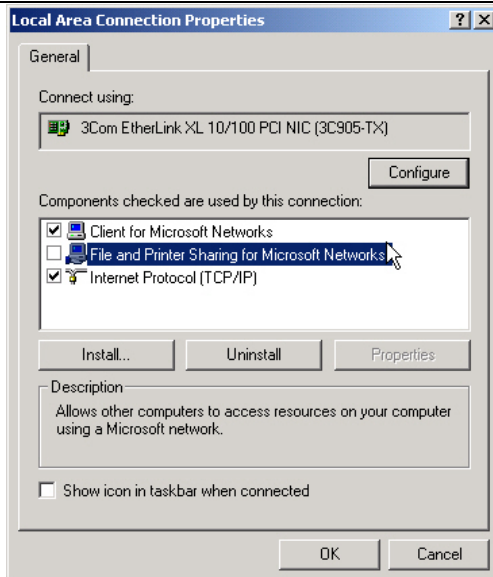
DHCP Configuration of TCP/IP in Windows NT4

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

1

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

2

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

The Network panel will display.

• Select the **Protocols** tab to continue.
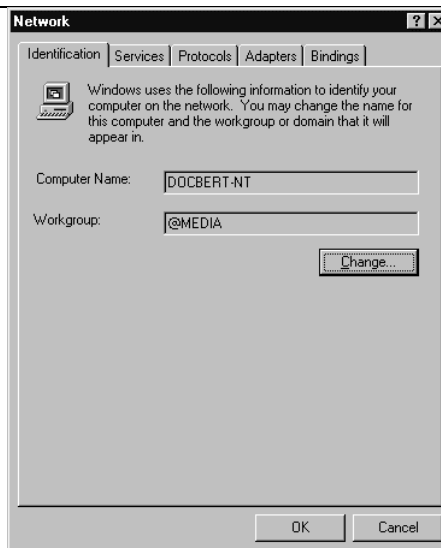
3

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

Network	? X
Identification	Services	Protocols	Adapters	Bindings

Network Protocols:

TCP/IP Protocol

Add...   Remove   Properties...   Update

Description:

OK   Cancel
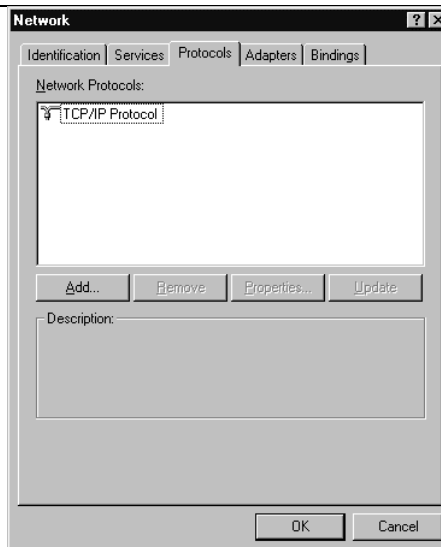
4

- The **TCP/IP Properties** dialog box now displays.

- Click the **IP Address** tab**.**

- Select the radio button marked **Obtain an IP address from a DHCP server.**

- Click **OK**. This completes the configuration of TCP/IP in Windows NT.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.
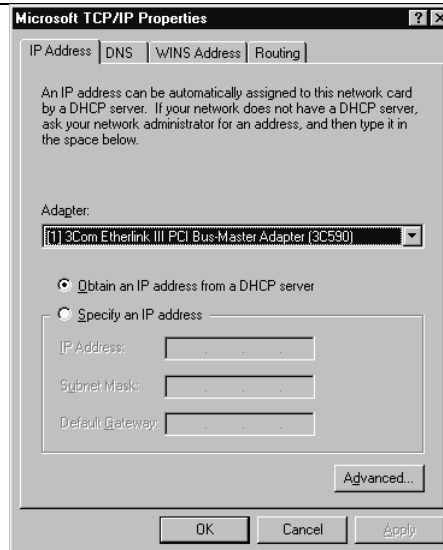
Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your PC's TCP/IP configuration:

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

   The Run window opens.

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

   A command window opens

3. Type **ipconfig /all**

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

   - The IP address is between 192.168.0.2 and 192.168.0.254

   - The subnet mask is 255.255.255.0

- • The default gateway is 192.168.0.1

4. Type **exit**

Configuring the Macintosh for TCP/IP Networking

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

MacOS 8.6 or 9.x

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

   The TCP/IP Control Panel opens:
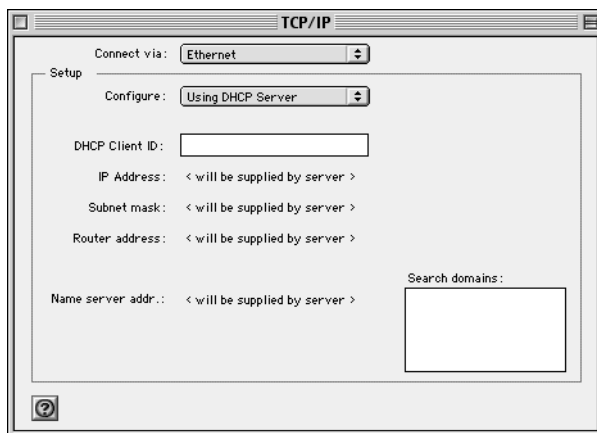
2. From the "Connect via" box, select your Macintosh's Ethernet interface.

3. From the "Configure" box, select Using DHCP Server.

   You can leave the DHCP Client ID box empty.

4. Close the TCP/IP Control Panel.

5. Repeat this for each Macintosh on your network.

MacOS X

1. From the Apple menu, choose System Preferences, then Network.

2.   If not already selected, select Built-in Ethernet in the Configure list.

3.   If not already selected, Select Using DHCP in the TCP/IP tab.

4.   Click Save.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.
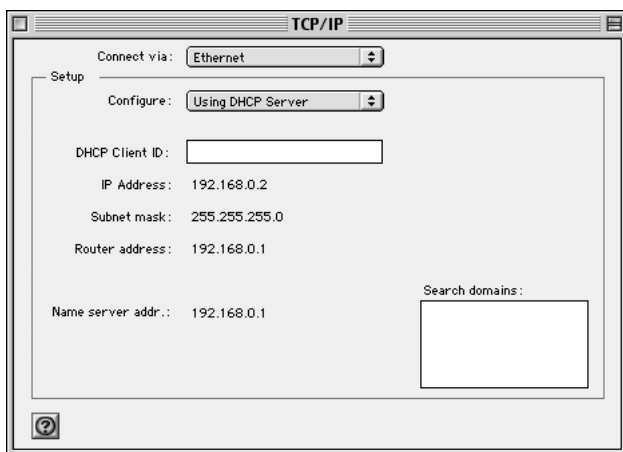
The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

•   The IP Address is between 192.168.0.2 and 192.168.0.254

•   The Subnet mask is 255.255.255.0

•   The Router address is 192.168.0.1

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 RP614 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 RP614 router. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

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

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

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

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

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

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

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

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

7.   Close the TCP/IP Control Panel.

Restarting the Network

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

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your RP614 router, you are ready to access and configure the firewall.

Glossary

10BASE-T	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
100BASE-Tx	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
802.11b	IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
ADSL	*See* Asymmetric Digital Subscriber Line
Asymmetric Digital Subscriber Line	A technology for sending data over regular telephone lines. ADSL allows data rates up to 8 Mbps downstream and 640 Kbps upstream.
Denial of Service attack	DoS. A hacker attack designed to prevent your computer or network from operating or communicating.
DHCP	*See* Dynamic Host Configuration Protocol.
DNS	*See* Domain Name Server.
Domain Name	A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.
Domain Name Server	A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
DSLAM	DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

Dynamic Host Configuration Protocol	DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.
Gateway	A local device, usually a router, that connects hosts on a local network to other networks.
IP	*See* Internet Protocol.
IP Address	A four-byte number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
IPSec	Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.
ISP	Internet service provider.
Internet Protocol	The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
LAN	*See* local area network.
local area network	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.
MAC address	Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.
Mbps	Megabits per second.
MSB	*See* Most Significant Bit or Most Significant Byte.
MTU	*See* Maximum Transmission Unit.
Maximum Transmit Unit	The size in bytes of the largest packet that can be sent or received.
Most Significant Bit or Most Significant Byte	The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.

NAT	*See* Network Address Translation.
Netmask	A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.
Network Address Translation	A technique by which several hosts share a single IP address for access to the Internet.
packet	A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.
PPP	*See* Point-to-Point Protocol.
PPPoA	*See* PPP over ATM
PPPoE	*See* PPP over Ethernet
PPP over ATM	PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
PPP over Ethernet	PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
PPTP	Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.
PSTN	Public Switched Telephone Network.
Point-to-Point Protocol	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
RFC	Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at www.ietf.org.
RIP	*See* Routing Information Protocol.
router	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
Routing Information Protocol	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

subnet mask	*See* netmask.
UTP	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.
VCI	Virtual Channel Identifier. Together with the VPI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.
VPI	Virtual Path Identifier. Together with the VCI, defines a Virtual Channel through an ATM network. Used by ATM switching equipment to route data through the network.
WAN	*See* wide area network.
WEP	Wired Equivalent Privacy. WEP is a data encryption protocol for 802.11b wireless networks. All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.
wide area network	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
Wi-Fi	*See* 802.11b. A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standard group promoting interoperability among 802.11b devices.
Windows Internet Naming Service	WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using Network Neighborhood.
WINS	*See* Windows Internet Naming Service.

Index

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com