Reference Manual for the Model DG814 DSL Modem Internet Gateway

NETGEAR

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

SM-DG814UK-0
April 2002

Trademarks

NETGEAR and FirstGear are trademarks Netgear, Inc.

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

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

Statement of Conditions

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

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

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

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

• Reorient or relocate the receiving antenna.

• Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/TV technician for help.

EN 55 022 Declaration of Conformance

This is to certify that the Model DG814 DSL Modem Internet 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 Model DG814 DSL Modem Internet 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 Model DG814 DSL Modem Internet 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 Model DG814 DSL Modem Internet 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.

Contents

Chapter 6
Maintenance

Chapter 7
Troubleshooting

About This Guide

Congratulations on your purchase of the NETGEAR™ Model DG814 DSL Modem Internet Gateway.

The Model DG814 gateway provides a secure connection for multiple personal computers (PCs) to the Internet through an internal ADSL modem that is normally intended for use by a single PC.

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

Technical Support

For help with any technical issues, contact Customer Support, 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.

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.

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)*.

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.

Caution: This format is used to highlight information that will help you prevent equipment failure or loss of data.

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.

Chapter 1
Introduction

This chapter describes the features of the NETGEAR Model DG814 DSL Modem Internet Gateway and discusses planning considerations for installation.

About the Router

The Model DG814 DSL Modem Internet Gateway with 4-port switch connects your local area network (LAN) to the Internet using a built-in ADSL modem.

The Model DG814 gateway provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day and address keywords, and share high-speed ADSL Internet access for up to 253 personal computers.

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

Key Features

The Model DG814 gateway provides the following features:

* Security
    – Parental control of web browsing using Web Address (URL) keyword blocking

    – Auditing and e-mail reporting of web browsing activities

    – Blocking can be scheduled by day and time

    – Network Address Translation (NAT) hides local PCs from the Internet

    – Incoming port forwarding and DMZ for specific services

- Built in 4-port 10/100 Mbps Switch
    - Allows LAN connections at 10 megabits per second (Mbps) or 100 Mbps
    - Autosensing for Ethernet (10BASE-T) or Fast Ethernet (100BASE-TX) transmissions
    - Autosensing MDI/MDIX configures each port for normal or uplink connection
    - Half-duplex or full-duplex operation
- Direct connection to the wide area network (WAN) using the built-in ADSL modem
- Protocol Support
    - IP routing
    - Dynamic extended Network Address Translation (NAT+) with port forwarding for operation with a single static or dynamic IP address
    - Dynamic Host Configuration Protocol (DHCP) server for dynamically assigning network configuration information to PCs on the LAN
    - DHCP client for dynamically obtaining configuration information from the Internet Service Provider (ISP)
    - DNS Proxy for simplified configuration
    - PPP over Ethernet (PPPoE) support
    - PPP over ATM (PPPoA) support
    - Classical IP support
- Login capability
    - Automatically executes user login for PPP over Ethernet or PPP over ATM accounts
- Easy, web-based setup for configuration
- Front panel LEDs for easy monitoring of status and activity
- Flash EPROM for firmware upgrade
- Free technical support seven days a week, twenty-four hours a day

Security

The Model DG814 gateway is equipped with several features designed to maintain security as described in this section.

- PCs Hidden by NAT
  Network address translation (NAT) opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.

- Port Forwarding with NAT
  Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the router allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated "DMZ" host computer.

Content Filtering

With its content filtering features, the Model DG814 gateway prevents objectionable content from reaching your PCs. Its content filtering features include:

- Content filtering by domain or keyword
  The Model DG814 gateway uses content filtering to enforce your network's Internet access policies. The gateway allows you to control access to Internet content by screening for keywords within Web URLs.

- Logging of inappropriate use
  You can configure the Model DG814 gateway to log access to Web sites and to e-mail the log to you. You can also configure the gateway to send an immediate alert e-mail message to you whenever a local user attempts to access a blocked Web site.

Autosensing 10/100 Ethernet

With its internal, 4-port 10/100 switch, the Model DG814 gateway can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The local LAN interface is autosensing and is capable of full-duplex or half-duplex operation.

The Model DG814 gateway incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a 'normal' connection (e.g. connecting to a PC) or an 'uplink' connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

TCP/IP

The Model DG814 gateway supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP).

For further information about TCP/IP, refer to Appendix B, "Networks and Routing Basics."

- IP Address Masquerading by Dynamic NAT+
  The Model DG814 gateway 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, an extension of Network Address Translation (NAT), is also known as IP address masquerading and allows the use of an inexpensive single-user ISP account.

- Automatic Configuration of Attached PCs by DHCP
  The Model DG814 gateway 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 LAN-attached PCs.

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

- PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA)
  PPPoE and PPPoA are protocols for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Easy Installation and Management

You can install, configure, and operate the Model DG814 DSL Modem Internet Gateway within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Animated installation assistant
  The Resource CD contains an animated installation assistant to guide you through set up.

- 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.

- Visual monitoring
  The Model DG814 gateway's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the Model DG814 gateway:

- Flash EPROM for firmware upgrade

- Free technical support seven days a week, twenty-four hours a day

Introduction

Chapter 2
Setting Up the Hardware

This chapter describes the Model DG814 DSL Modem Internet Gateway hardware and provides instructions for installing it.

Package Contents

The product package should contain the following items:

- Model DG814 DSL Modem Internet Gateway
- AC power adapter, 18 V AC output (varies by region)
- Category 5 (Cat 5) Ethernet cable, straight-through wiring
- Telephone cable
- Microfilters (quantity and type vary by region)
- *Model DG814 Resource* CD, including:

    — This guide

    — Application Notes

- *DG814 DSL Modem Internet Gateway Installation Guide*
- Warranty Card
- Support Information Card

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

Local Network Hardware Requirements

The Model DG814 DSL Modem Internet Gateway is intended for use in a network of personal computers (PCs) that are interconnected by twisted-pair Ethernet cables.

PC Requirements

To install and run the Model DG814 gateway over your network of PCs, each PC must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the PC will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the cable provided with your router.

Access Requirement

The Model DG814 DSL Modem Internet Gateway contains a built-in ADSL modem, which connects directly to an ADSL service provider.

The Router's Front Panel

The front panel of the Model DG814 gateway (Figure 2-1) contains status LEDs.
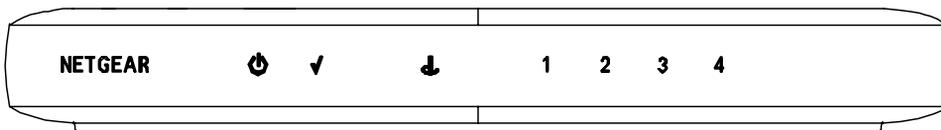
Figure 2-1.   DG814 Front Panel

You can use some of the LEDs to verify connections. Table 2-1 lists and describes each LED on the front panel of the Model DG814 gateway. These LEDs are green when lit.

Table 2-1.   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.
ADSL (Wide Area Network)	On (Green) Blink (Green) Blink (Yellow) Off	The ADSL port has linked with the service provider. Data is being transmitted or received over the ADSL port. The ADSL port is attempting to train with the service provider. The ADSL port is not making contact with the service provider.
Local (Local Area Network) 4	On (Green) Blink (Green) On (Yellow) Blink (Yellow) 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 Router's Rear Panel

The rear panel of the Model DG814 gateway (Figure 2-2) contains port connections and a power switch.
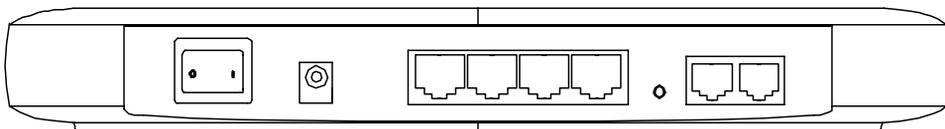
Figure 2-2.   DG814 Rear Panel

The rear panel contains the following features (from left to right):

• Power switch

• 18 V AC power adapter outlet

• Four Local (LAN) Ethernet ports for connecting the router to the local PCs

• Factory Default Reset push-button

• ADSL (WAN) port, with two identical connectors, for connecting the router to the ADSL service provider. One of the ports can be connected to a telephone using an external microfilter.

Connecting the Router

Before using your gateway, you need to do the following:

• Connect your local Ethernet network to the Local port(s) of the gateway (see page 2-5).

• Connect the line from your ADSL service provider to the ADSL port of the gateway (see page 2-6).

• Connect the power adapter (see page 2-7).

A typical installation is shown in Figure 2-3, below
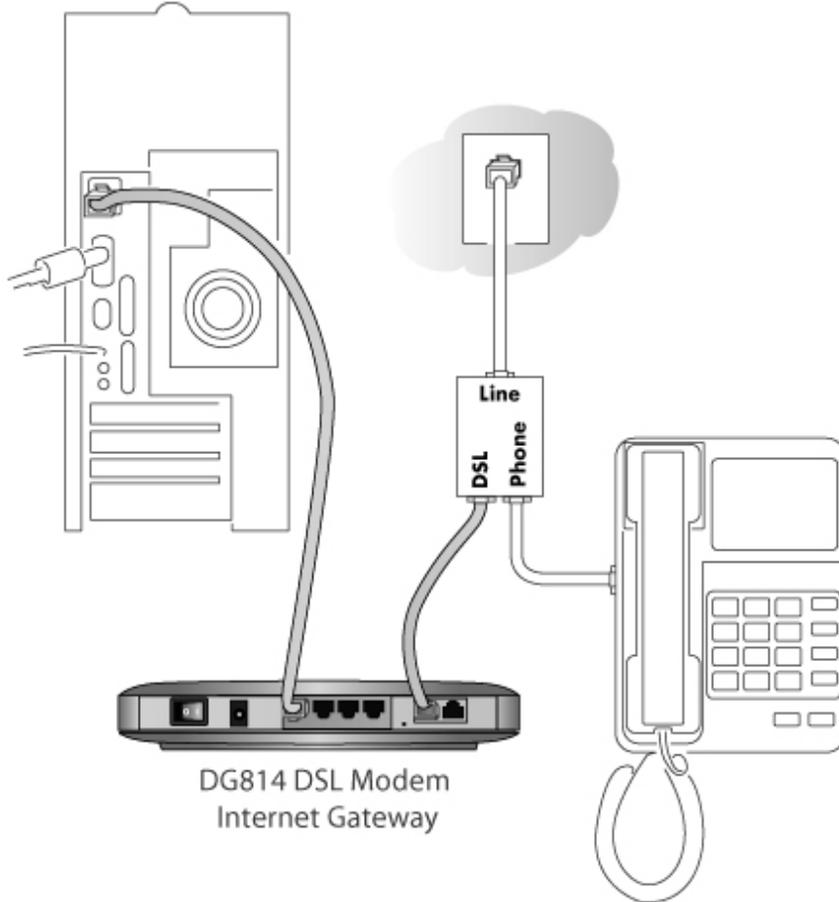
Figure 2-3.   Typical installation

Connecting to your Local Ethernet Network

Your local network (LAN) will attach to the four Local router ports shown in Figure 2-2. The Local ports operate at either 10 Mbps (10BASE-T) or 100 Mbps (100BASE-Tx), depending on the Ethernet interface of the attached PC, hub, or switch. For any connection which will operate at 100 Mbps, you must use a Category 5 (Cat 5) rated Ethernet cable, such as the cable included with the router.

The Model DG814 gateway incorporates a four-port switch for connecting to your local network. To connect the Model DG814 gateway to your LAN:

• Connect up to four PCs directly to any of the four Local ports of the router using standard Ethernet cables.

If your local network consists of more than four computers, you will need to connect your router to another hub or switch:

• Connect any Local port of your router to any port of an Ethernet hub or switch using a standard or crossover Ethernet cable.

 Because the gateway incorporates Auto Uplink™ technology (also called Auto MDI/MDI-X), it is capable of automatically sensing the polarity of the Ethernet connection. You can therefore connect to the other hub's normal or uplink port using a standard or crossover Ethernet cable. The Local port of your Model DG814 gateway will automatically configure itself properly.

Connecting to Your ADSL Service and Telephone Provider

The ADSL and telephone connections may vary by region.

ADSL through a modular RJ-11 wall jack.

	Note: The wall jack attached to the ADSL port of the router must provide the ADSL signal on the inner pair of wires (pins 2 and 3 of the 4-pin jack). If this is not the case, a swapper (not included) is necessary to move the connection to the inner pair.

To install the Model DG814 gateway directly to the wall jack without installing a telephone:

1. Connect the provided telephone cable to the wall jack.

2. Connect the other end of the telephone cable to the ADSL port on the router.

To install both the Model DG814 gateway and a telephone:

1. Plug the "LINE" connection from the included microfilter into the wall jack.

2. Connect the "DSL" jack of the microfilter to the ADSL port of your router using the telephone cable provided.

3. Connect the "PHONE" side of the microfilter to your telephone, using your existing telephone cable.

ADSL through other wall jacks

1. Plug the "LINE" connection from the included microfilter into the wall jack.

2. Connect the "DSL" jack of the microfilter to the ADSL port of your router using the telephone cable provided.

3. Connect the "PHONE" side of the microfilter to your telephone, using your existing telephone cable.

A telephone can be attached to the second RJ-11 jack on your router. However, a microfilter should be connected between the router and the telephone. Be careful to connect the microfilter according to its markings, with the "LINE" side plugged into the router and the "PHONE" side connected to your telephone.

If you have additional telephones, you will need to purchase additional microfilters and connect them between the telephones and the wall jack. A microfilter is required for each telephone on the line.

> **→** **Note:** Microfilters are required to isolate your ADSL signal from your telephone signal. If microfilters are not used, or if they are connected backward, you may notice a "ticking" noise on your telephone, and the performance of your ADSL line may be affected.

Connecting the Power Adapter

To connect the power adapter to the gateway:

1. Plug the connector of the power adapter into the 18 V AC adapter outlet on the rear panel of the router.

2. Plug the other end of the adapter into a standard wall outlet.

3. Set the gateway's Power switch to the ON position.

4. Verify that the PWR LED on the router is lit.

Verifying Power

After applying power to the gateway, complete the following steps to verify that power is correctly applied:

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

All LEDs will briefly be tested.

2. After approximately 10 seconds, verify that:

    •   The Test LED is not lit.

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

3. If a port's LED is lit, a link has been established to the connected device. If a Local port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED should be yellow.

You are now ready to begin configuration of your network, as described in the following chapter.

Chapter 3
Preparing Your Network

This chapter describes how to prepare your PC network to connect to the Internet through the Model DG814 DSL Modem Internet Gateway and how to order broadband Internet service from an Internet service provider (ISP).

> ➡ **Note:** If an ISP technician configured your PC 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 gateway. Refer to "Obtaining ISP Configuration Information (Windows)" on page 3-10 or "Obtaining ISP Configuration Information (Macintosh)" on page 3-11 for further information.

Preparing Your Personal Computers for IP Networking

Personal Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). Each PC 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.

Note: In this chapter, we use the term "PC" to refer to personal computers in general, and not necessarily Windows computers.

Most operating systems include the software components you need to install and use TCP/IP on your PC:

- Windows® 95 or later (including Windows NT®) 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 PCs and the gateway must be assigned 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 and Routing Basics.""

The Model DG814 gateway is shipped preconfigured as a DHCP server. The gateway 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 gateway)—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 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:
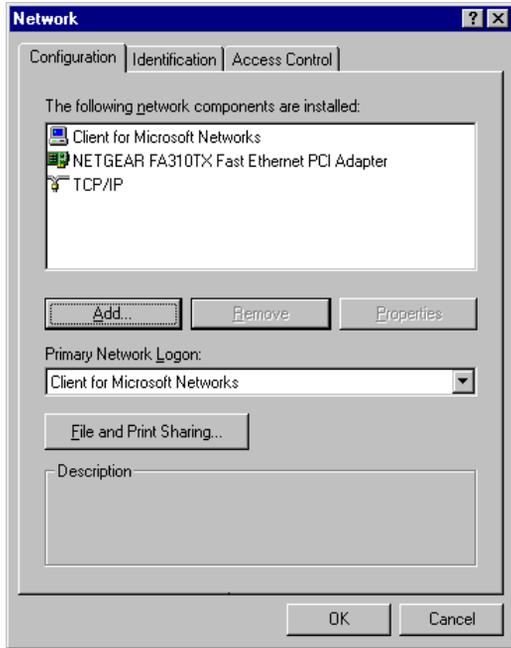
You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

→	**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 the adapter:

1. Click the Add button.
2. Select Adapter, and then click Add.
3. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

1. Click the Add button.
2. Select Protocol, and then click Add.
3. Select Microsoft.
4. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

1. Click the Add button.

2. Select Client, and then click Add.

3. Select Microsoft.

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

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

Assign TCP/IP configuration by DHCP

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 the internal DHCP server of the Model DG814 gateway. To use DHCP with the recommended default addresses, follow these steps:

1. Connect all PCs to the router, then restart the gateway and allow it to boot.

2. On each attached PC, open the Network control panel (refer to the previous section) and select the Configuration tab.

3. From the components list, select TCP/IP->(your Ethernet adapter) and click Properties.

4. In the IP Address tab, select "Obtain an IP address automatically".

5. Select the Gateway tab.

6. If any gateways are shown, remove them.

7. Click OK.

8. Restart the PC.

Repeat steps 2 through 8 for each PC on your network.

Selecting 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 (Windows)

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:

    *   The IP address is between 192.168.0.2 and 192.168.0.253

    *   The subnet mask is 255.255.255.0

    *   The default gateway is 192.168.0.1

Configuring Windows NT or 2000 for 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 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.   Make sure your PC is connected to the router, then reboot your PC.

Verifying TCP/IP Properties

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:

- 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 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 by following these steps:

Mac OS 7, 8.6 or 9.x

1. From the Apple menu, choose Control Panels, and then chooseTCP/IP.

    The TCP/IP control panel opens:
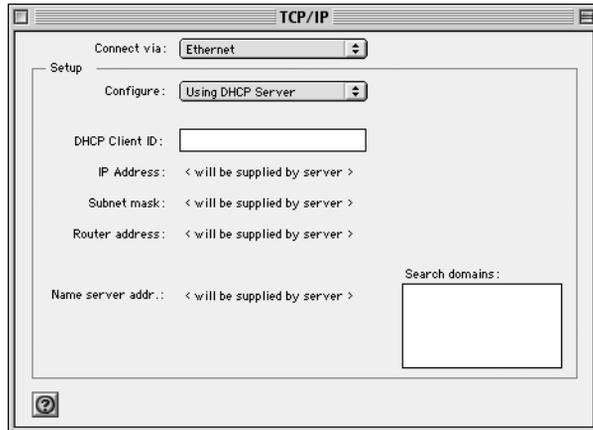
2. If not already selected, select Ethernet in the "Connect via" list.
3. Select Using DHCP Server in the "Configure" list.
4. Click the Close box
5. Click Save.
6. Repeat this for each Macintosh on your network.

Mac OS X

1. Choose System Preferences from the Apple menu.
2. Double-click Network.
3. If not already selected, select Built-in Ethernet in the "Configure" list.
4. If not already selected, select Using DHCP in the TCP/IP tab.
5. Click Save
6. Repeat this for each Macintosh on your network.

Verifying TCP/IP Properties (Macintosh)

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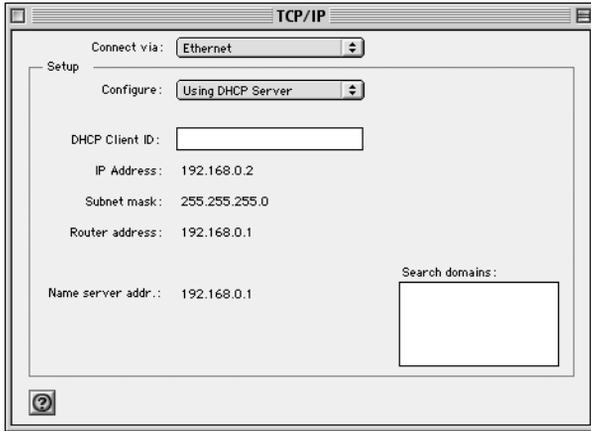
The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- 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".

Your Internet Account

For access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using ADSL. The Model DG814 DSL Modem Internet Gateway includes a built-in ADSL modem that connects directly to your ADSL line.

For a single-user Internet account, your ISP supplies TCP/IP configuration information (such as IP address, subnet mask and default gateway) and VPI and VCI multiplexing information for one PC. Your ISP may also provide other login information, such as User Name and Password, in the case where the PPPoE or PPPoA protocol is required. 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 gateway 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 gateway's ADSL port is connected, the gateway appears to be a single PC to the ISP. The gateway 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 gateway to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Login Protocols

Some ISPs require special login protocols. In this case, you will need to know what type of protocol is used, and you will need a login name and password. The two common protocols are:

*   PPP over Ethernet (PPPoE)
    Two common PPPoE clients are WinPOET and EntreNet.

*   PPP over ATM (PPPoA)

After your network and gateway are configured, the gateway will perform the login task when needed, and you will no longer need to login from your PC.

Account Information

Unless these items are dynamically assigned by the ISP, your ISP should give 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 gateway 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 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 gateway. These procedures are described next.

Obtaining ISP Configuration Information (Windows)

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the Model DG814 gateway. 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 gateway 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 (Macintosh)

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the Model DG814 gateway. 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 gateway 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.

Ready for Configuration

After configuring all of your PCs for TCP/IP networking and connecting them to the LOCAL network of your Model DG814 gateway, you are ready to access and configure the gateway. Proceed to the next chapter.

Preparing Your Network

Chapter 4
Basic Configuration of the Router

This chapter describes how to perform the basic configuration of your Model DG814 DSL Modem Internet Gateway using the Setup Wizard which walks you through the configuration process for your Internet connection.

Configuring for Internet Access

In order to use the browser-based Web Configuration Manager, your PC must have a web browser program installed such as Microsoft Internet Explorer or Netscape Navigator. Because the Configuration Manager uses Java, your Web browser must be Java-enabled and support HTTP uploads. NETGEAR recommends using Netscape Navigator 3.0 or above. Free browser programs are readily available for Windows, Macintosh, or UNIX/Linux.

To configure for Internet access using your browser:

1. Turn on the router and wait for initialization to complete.

   Allow at least one minute and verify that the TEST LED is off. ✓

2. Reboot your PC to obtain DHCP configuration from the router.

3. Launch your web browser.

4. In the Address box of your browser, type **http://192.168.0.1** and press ENTER.

A login window opens as shown in Figure 4-1 below:.

Figure 4-1.   Login window

This screen may have a different appearance in other browsers.

5.   Type **admin** in the User Name box, **password** in the Password box, and then click OK.

If your gateway password was previously changed, enter the current password.

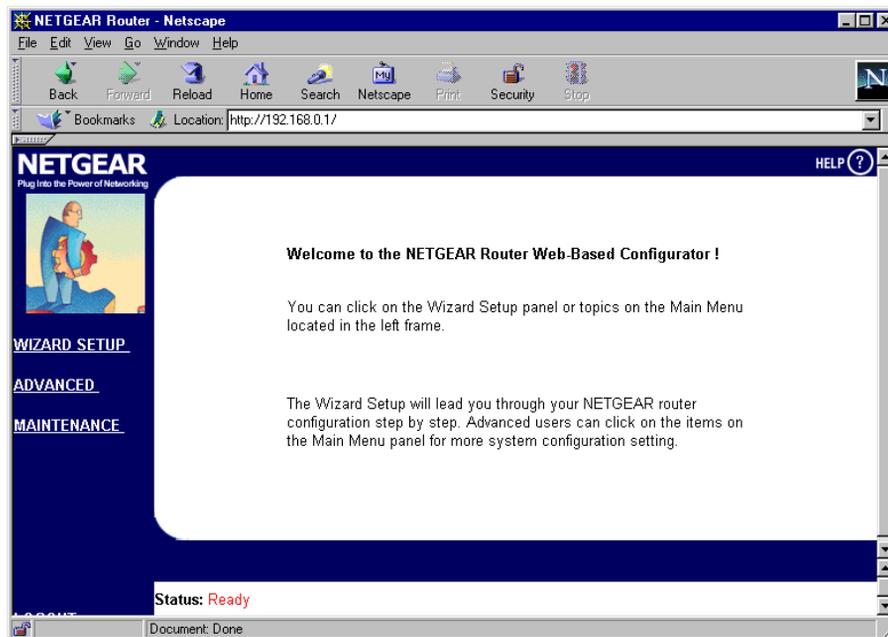6.   In the opening screen, shown in Figure 4-2, select WIZARD SETUP.

Figure 4-2.   Browser-based configuration main menu

7. In the first Wizard screen, enter your account's System Name and Domain Name, as shown in Figure 4-3 below:

Figure 4-3.   Browser-based Setup Wizard, first screen

These parameters may be necessary to access your ISP's services such as mail or news servers. If your ISP does not provide a System or Host name leave this field blank. If you leave the Domain Name field blank, the router will attempt to learn the domain automatically from the ISP. If this is not successful, you will need to enter it manually.

8. Click Next to go to the ISP Parameters screen, shown in Figure 4-4 below.

Figure 4-4.   Browser-based Setup Wizard, second screen

Your ISP will indicate whether your Multiplexing Method is VC-BASED or LLC-BASED and which VPI and VCI is used. Enter the information in this screen. The most common Multiplexing Method is LLC-based. If your service provider does not indicate which one is used, use LLC-BASED.

9. Click Next to go to the second ISP Parameters screen, shown in Figure 4-5 below:

ISP Parameters for Internet Access

Encapsulation	PPP over Ethernet ▾
Service Name	
User Name	
Password	
Idle Timeout	0 Minutes.

Back Next

Figure 4-5.   Browser-based Setup Wizard, third screen

This screen determines whether a login program will be run.

*   If your service provider does not require a login program, leave Encapsulation as Ethernet. It is not necessary to enter a Service Type, User Name, or Password. Proceed to Step 3.

*   If your service provider uses PPP over Ethernet (PPPoE), select Encapsulation as PPP over Ethernet, and enter these additional parameters:

    1. If your connection supports multiple ISPs, enter the Service Name of the one you use. Otherwise leave Service Name blank.

    2. Enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive.

    3. If you wish to change the login timeout, enter a new value in minutes.

    Proceed to Step 3.

*   If your service provider uses PPP over ATM (PPPoA), select Encapsulation as PPP over ATM, and enter these additional parameters:

    1. Enter the PPPoA login user name and password provided by your ISP. These fields are case sensitive.

2. If you wish to change the login timeout, enter a new value in minutes.

- If your service provider uses Classical IP, select Classical IP. It is not necessary to enter a Service Type, User Name, or Password. Proceed to Step 3..

> **Note:** PPPoE and PPPoA will authenticate with the network when you have data to transmit.The gateway will stay connected until you stop transmitting and will then wait for the login timeout to expire before disconnecting.

3. Click Next to go to the final Wizard screen shown in Figure 4-6 below.

WAN IP Address Assignment

- ⦿ **Get automatically from ISP (Default)**
- ○ **Use fixed IP address**
  - **IP Address**   `0.0.0.0`
  - **IP Subnet Mask**   `255.255.255.0`
  - **Gateway IP Address**   `0.0.0.0`

DNS Server Address Assignment

- ⦿ **Get automatically from ISP (Default)**
- ○ **Use fixed IP address --- DNS Server IP Address**   `0.0.0.0`

`Back`

Figure 4-6.   Browser-based Setup Wizard, fourth screen

This screen provides setup for the following parameters:

- WAN IP Address Assignment: Unless your ISP has assigned a fixed permanent IP address for your use, select "Get automatically from ISP" to obtain and IP address using DHCP. Otherwise, enter your IP Address, Subnet Mask, and the IP Address of your ISP's gateway router.

- DNS Server Address Assignment: If you know that your ISP does not automatically transmit DNS addresses to the router during login, select "Use fixed IP address" and enter the IP address of the ISP's DNS server.
  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP transfers the IP addresses of one or two DNS servers to your router 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 router.

4. Click Finish.

5. Click the NETGEAR website address to test your Internet connection.

    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. When your router and PCs are configured correctly, your router automatically accesses the Internet when one of your LAN devices requires access. It is not necessary to run a dialer application such as Dial-Up Networking or PPPoE or PPPoA Login to connect, log in, or disconnect. These functions are performed by the router as needed.

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

Configuring for Content Filtering

The Model DG814 DSL Modem Internet Gateway provides you with Web content filtering options, plus browsing activity reporting and instant e-mail alerts. Parents and network administrators can establish restricted access policies based on time-of-day, web addresses and web address keywords.

To configure these features of your router, click the Advanced heading in the Main Menu of the browser interface. From the subheadings shown, click CONTENT FILTER. The tabs described below contain the settings for the content filtering.

E-Mail

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

- Turn E-mail Notification On
  Check this box to enable the e-mail notification feature.

- Mail Server
  Specifies the name of your outgoing (SMTP) mail server. You can enter either the server name (such as mail.myISP.com) or its IP Address.

- E-mail To
  Specifies the e-mail address to which logs and alerts are sent. This e-mail address will be used as the From address, as well. If you leave this box blank, the log is not sent via e-mail to any address.

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

- Send immediate alert upon attempted access to a blocked site
  Check this box if you would like immediate notification of inappropriate access attempts.

- Log 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, using 23:59 notation. Relevant when the log is sent daily.

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

- Adjust for Daylight Savings Time
  The gateway does not automatically adjust for daylight savings time. Check this box if you are currently on daylight savings time.

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 router overwrites the log and discards its contents.

The Model DG814 gateway uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. This menu displays the current time.

Keyword

The Model DG814 gateway allows you to restrict access based on web addresses and web address keywords. Up to 255 entries are supported in the Keyword list. The Keyword tab is shown below.

To enable keyword blocking, check Enable Keyword Blocking, then click Apply. Be sure that a time period for blocking is specified on the Schedule setup screen.

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

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

Keyword application examples:

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

Schedule

The Model DG814 gateway allows you to specify when blocking will be enforced. The Schedule tab is shown below.

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

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

Trusted

The Model DG814 gateway allows you to 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.

The Trusted tab is shown below.

To specify a Trusted Host, enter the Trusted Host's IP address in the Trusted Device box and click Apply.

Logs

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

```
  E-mail      Keyword      Schedule      Logs

               Content Filter Logs (Page 1/1)
No. Time & Entry            Source IP          Action
  0|Thu, 22 Feb 2001 23:09:40 |192.168.0.33     |BLOCK_KEYWORD
    www.playboy.com
  1|Thu, 22 Feb 2001 23:09:31 |192.168.0.33     |FORWARD
    us.a1.yimg.com
  2|Thu, 22 Feb 2001 23:09:31 |192.168.0.33     |FORWARD
    us.a1.yimg.com
  3|Thu, 22 Feb 2001 23:09:30 |192.168.0.33     |FORWARD
    www.yahoo.com



         Previous Page   Refresh   Clear   Next Page
```

Log entries are described in Table 4-1

Table 4-1.   Content Filter Log entry descriptions

Field	Description
No.	The index number of the content filter log entries. 128 entries are available numbered from 0 to 127. The log will keep the record of the latest 128 entries.
Time and Entry	The date and time the log entry was recorded. Below the date and time is the name or IP address of the website visited or attempted to access.
Source IP	The IP address of the initiating device for this log entry.
Action	This field displays whether the packet was blocked or forwarded (BLOCK or FORWARD).

Log viewing buttons are described in Table 4-2

Table 4-2.   Log display buttons

Field	Description
Previous Page	Click this button to view the previous log page.
Refresh	Click this button to refresh the log screen.
Clear	Click this button to clear the log entries.
Next Page	Click this button to view the next log page.

Chapter 5
Advanced Configuration of the Router

This chapter describes how to configure the advanced features of your Model DG814 DSL Modem Internet Gateway. These features can be found by clicking on the Advanced heading in the Main Menu of the browser interface. One advanced feature, Content Filtering, is described in the previous chapter.

System Settings

The first feature category under the Advanced heading is SYSTEM settings. These are general purpose settings.

System Tab

The System Tab contains fields for setting the System (Host) Name and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers.

- System Name
  This is the host or account name given by your ISP for naming your PC. It is often the primary e-mail name of your account.This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.

- Domain Name
  This is the extended domain suffix that follows your ISP server names. For example, if your ISP's mail server is mail.sfbay.myISP.com, then your Domain Name is sfbay.myISP.com.

Dynamic DNS

Your router supports Dynamic Domain Name Service (DDNS). In a Dynamic DNS service, an IP registry server provides a public central database where dynamically-assigned IP addresses can be stored and retrieved by hostname lookup. The Dynamic DNS server also stores password-protected e-mail addresses along with IP addresses and hostnames and accepts queries based on e-mail addresses.

To utilize this service, you must register with the Dynamic DNS service provider, who will give you a password or key. At this time, the Model DG814 gateway only supports DynDNS service. For more information, visit www.dyndns.org.

The configuration fields for Dynamic DNS are shown in Table 5-1:

Table 5-1.   Dynamic DNS configuration fields

Field	Description
Active	Use this field to activate or deactivate dynamic DNS registration.
Service Provider	Select a dynamic DNS service provider.
Host Name	Enter the static host name that will link to your dynamic IP address.
Domain Name	Enter the domain name.
User	Enter the user name of your dynamic DNS account.
Password	Enter the password of your dynamic DNS account.
Enable Wildcard	DynDNS.org allows the use of wildcards in resolving your URL. Enabling the wildcard feature for your host will cause ***.yourhost.dyndns.org** to be aliased to the same IP address as **yourhost.dyndns.org**.

For example, to register **yourhost.dyndns.org**, enter **yourhost** for the Host Name and **dyndns.org** for the Domain Name.

Password

Select the Password tab to change your router's management password. This is the password to access the router for configuration, not for Internet access. To change the password, first enter the old password, and then enter the new password twice. Click Apply.

LAN Setup

The second feature category under the Advanced heading is LAN SETUP. This menu allows configuration of LAN IP services such as DHCP and RIP. From the Main Menu of the browser interface, under Advanced, click LAN to view the LAN SETUP menu, shown in Figure 5-1, below.
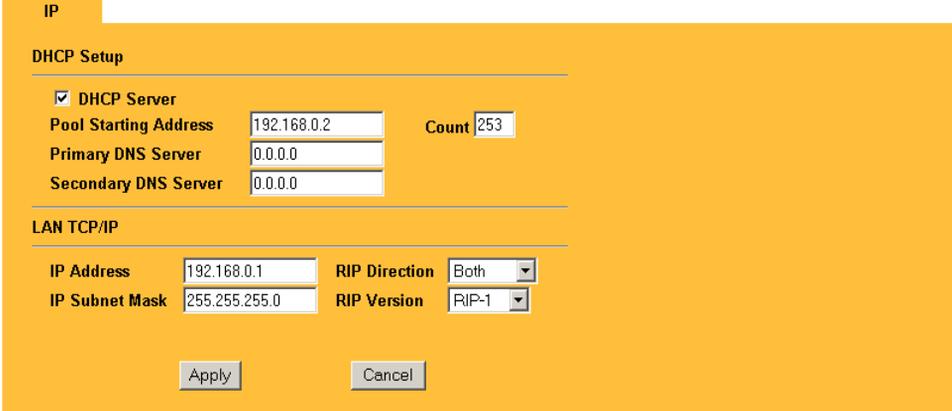
Figure 5-1.   LAN Setup Menu

DHCP

The Model DG814 gateway has the capability to act as a DHCP server, allowing it to assign IP, DNS, and default gateway addresses to attached PCs. The assigned default gateway address is the LAN address of the router. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

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.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. These default settings are:

• DHCP server enabled with 253 client addresses starting from 192.168.0.1.

Table 5-2 lists and describes the fields to use for setting up DHCP parameters.

Table 5-2. **DHCP Setup Fields**

Field	Description
DHCP Server:	If this box is checked, the router acts as a DHCP server. If this box is cleared, the router's DHCP server is disabled.
Pool Starting Address	The beginning of the range of IP addresses to assign.
Count	The number of sequential addresses available for assignment to attached hosts. The maximum is 253.
Primary DNS Server	If you want the router to provide the Primary DNS Server address to attached hosts, enter the DNS address in this field. If this field is 0.0.0.0, the router assigns its own address as DNS Server, and performs a DNS Proxy if it can obtain a DNS address from the ISP.
Secondary DNS Server	If you want the router to assign the Secondary DNS Server address to attached hosts, enter the address in this field.

LAN TCP/IP

Table 5-3 lists and describes the fields to use for setting up TCP/IP parameters for the LAN..

Table 5-3. **LAN TCP/IP Setup Fields**

Field	Description
TCP/IP Setup:	
IP Address	Enter the IP address of the LAN interface of the router in dotted-decimal notation (four 8-bit numbers, between 0 and 255, separated by periods, for example, 192.168.0.1). Every device on the TCP/IP network must have a unique IP address.
IP Subnet Mask	An IP address consists of two parts, the network ID and the host ID. The IP Subnet Mask specifies the network ID portion of the address, written in dotted-decimal notation. The router automatically calculates this mask for the class of the IP address that you assign. Unless you have a special need for subnetting, use the default subnet mask calculated by the router. All hosts on the LAN segment should use the same mask.

Table 5-3.   LAN TCP/IP Setup Fields (continued)

Field	Description
RIP Direction	This parameter determines how the router handles RIP (Routing Information Protocol). RIP allows the router to exchange routing information with other routers. If set to None (default), the router does not participate in any RIP exchange with other routers. If set to Both, the router broadcasts the routing table of the router on the LAN and incorporates RIP broadcasts by other routers into its routing table. If set to In Only, the router broadcasts its routing table on the LAN. If set to Out Only, the router broadcasts its routing table, but it ignores any RIP broadcast packets that it receives. Usually, you should leave this parameter at the default (None).
RIP Version	This field determines the format and broadcasting method of any RIP (Routing Information Protocol) transmissions by the router. The following RIP options are supported by the Model DG814 gateway: • RIP-1—The router sends RIP-1 messages only. • RIP-2B—The router sends RIP-2 messages in broadcast format. • RIP-2M—The router sends RIP-2 messages in multicast format. For most applications, the recommended version is RIP-1.

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

Configuring for Port Forwarding to Local Servers

Although the router causes your entire local network to appear as a single machine to the Internet, you can make local servers for different services (for example, FTP or HTTP) visible and available to the Internet. This is done using the PORTS menu. From the Main Menu of the browser interface, under Advanced, click PORTS to view the port forwarding screen, shown in Figure 5-2.

Figure 5-2.   Port Forwarding Menu

Requested services are identified by port numbers in an incoming IP packet. For example, a packet that is sent to the external IP address of your router and destined for port number 80 is an HTTP (Web server) request, and port 21 is an FTP request. Examples of port numbers are shown at the top of the PORTS menu, although you are not limited to these choices. See IETF RFC1700, "Assigned Numbers," for port numbers for common protocols.

> **Note:** Many 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.

Use the PORTS menu to configure the router to forward incoming protocols to IP addresses on your local network based on the port number. In addition to servers for specific protocols, you can also specify a Default (also called DMZ) Server to which all other incoming protocols are forwarded. To configure port forwarding to a local server:

1. Enter the Port Number in an unused Start Port box.

2. To forward only one port, enter it again in the End Port box. To specify a range of ports, enter the last port to be forwarded in the End Port box.

3. Enter the IP address of the local server in the corresponding Server IP Address box.

4. Click Apply at the bottom of the menu.

Local Web and FTP Server Example

If a local PC, with a private address of 192.168.0.33, acts as a Web and FTP server, configure the PORTS menu to forward ports 80 (HTTP) and 21 (FTP) to local address 192.168.0.33 as shown in Table 5-4.

Table 5-4.   Port Table Entries (Example)

Port #	Server IP Address
Default	0.0.0.0
80 (HTTP)	192.168.0.33
21 (FTP)	192.168.0.33

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

Some considerations for this application are:

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

• If the IP address of the local PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, change the configuration of your PCs to use fixed private addresses rather than DHCP-assigned addresses.

- Local PCs must access the local server using the PCs' local LAN address (192.168.0.33 in this example). Attempts by local PCs to access the server using the external IP address (172.16.1.23 in this example) will fail.

Local Game Host or Videoconference Example

Some online games and videoconferencing applications are incompatible with NAT. The Model DG814 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 in the PORTS Menu. If one local PC acts as a game or videoconference host, enter its IP address as the default.

Static Routes

The fourth feature category under the Advanced heading is STATIC ROUTE, which allows configuration of additional routing information. 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.

From the Main Menu of the browser interface, under Advanced, click STATIC ROUTE to view the IP Static Route menu, shown in Figure 5-3.

Figure 5-3.   IP Static Route Summary Table

To add or edit a Static Route, select a number and click the Edit button to open the Edit Menu, shown in Figure 5-4, below.

Figure 5-4.   Static Route Entry and Edit Menu

Table 5-5 lists and describes the fields for the IP Static Route Edit menu.

Table 5-5.   Edit IP Static Route Fields

Field	Description
Route Name	Enter a descriptive name for this route for identification purposes only.
Destination IP Address	Enter the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway to the destination network. The gateway is the next router that your router contacts in order to forward packets to the destination. On the LAN, the gateway must be a router on the same segment as the router. Over the WAN, the gateway will be the IP address of the router at your ISP.
Metric	Enter the cost in 'hops' of transmission for routing purposes. IP routing uses hop counts as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number does not have to be precise, but it must be between 1 and 16. In practice, 2 or 3 is usually a good number.
Private	Use this field to determine whether the router includes the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in any RIP broadcast. If set to No, the route to this remote node is propagated to other hosts through RIP broadcasts.

Static Route Example

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

- Your primary Internet access is through the Model DG814 gateway 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.x.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.100. The static route would look like Figure 5-5, below.

Figure 5-5.   Static Route Example

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 either 1 or 2 will work.

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

Chapter 6
Maintenance

This chapter describes how to use the maintenance features of your Model DG814 DSL Modem Internet Gateway. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

System Status

The System Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, click Maintenance, then select SYSTEM STATUS to view the System Status screen, shown in Figure 6-1.
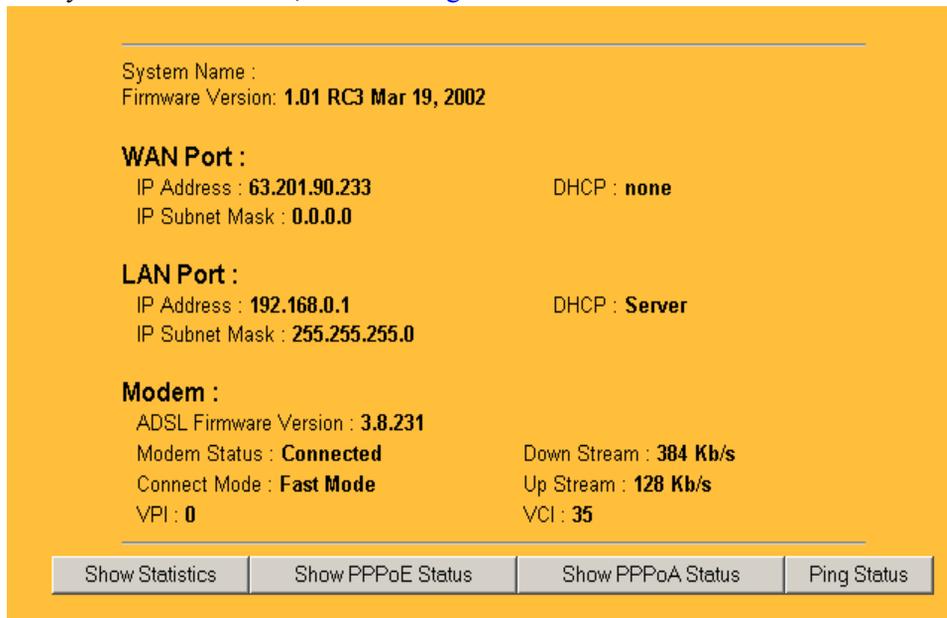

Figure 6-1.   **System Status screen**

The System Status screen shows the parameters listed in

Table 6-1. **System Status fields**

Field	Description
System Name	This field displays the Host Name assigned to the router.
Router Firmware Version	This field displays the router firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the router.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router.
DHCP	If set to None, the router is configured to use a fixed IP address on the WAN or to use PPPoE or PPPoA. If set to Client, the router is configured to obtain an IP address dynamically from the ISP.
LAN Port	These parameters apply to the Local (LAN) port of the router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the router. 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 router. The default is 255.255.255.0
DHCP	If set to None, the router will not assign IP addresses to local PCs on the LAN. If set to Server, the router is configured to assign IP addresses to local PCs on the LAN.
ADSL Firmware Version	This field displays the ADSL chipset firmware version.
Modem Status	This field displays the state of the ADSL connection to your service provider, either "Connecting" or "Connected"
Connect Mode	This field displays the protocol used to connect to your service provider. When the ADSL link comes up, the connection will be either "Fast" or "Interleaved", depending on the way the telephone company has configured its equipment
Down Stream	This field displays the connection rate in from the service provider to the router in bits per second
Up Stream	This field displays the connection rate in from the router to the service provider in bits per second
VPI	This field displays the VPI entered in the WIZARD SETUP
VCI	This field displays the VCI entered in the WIZARD SETUP

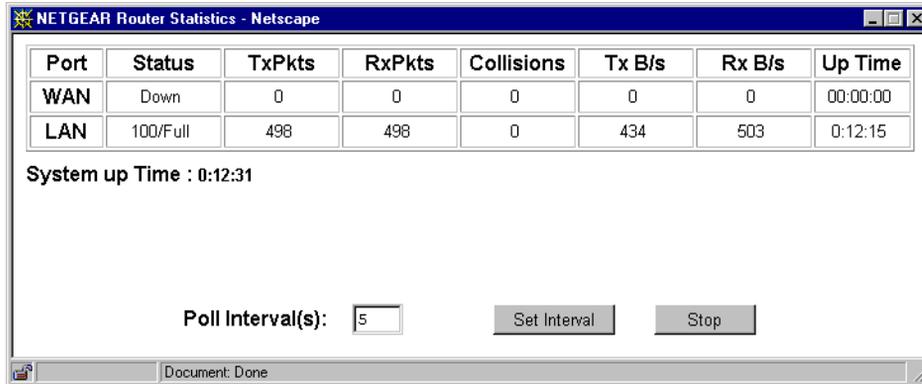Click the "Show Statistics" button to display router usage statistics, as shown in Figure 6-2 below.:

Figure 6-2.   Router Statistics screen

This screen shows the following statistics:.

Table 6-2.   Router Statistics Fields

Field	Description
Port	The statistics for the WAN (Internet) and LAN (local) ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The average line utilization, measured in Bytes transmitted per second, over the Poll Interval specified.
Rx B/s	The average line utilization, measured in Bytes received per second, over the Poll Interval specified.
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 interval (in seconds) at which the statistics are updated in this window. Click Stop to freeze the display.

Click the "PPPoE Status" or "PPPoA Status" button to check the status in detail, as shown in Figure 6-3, below.
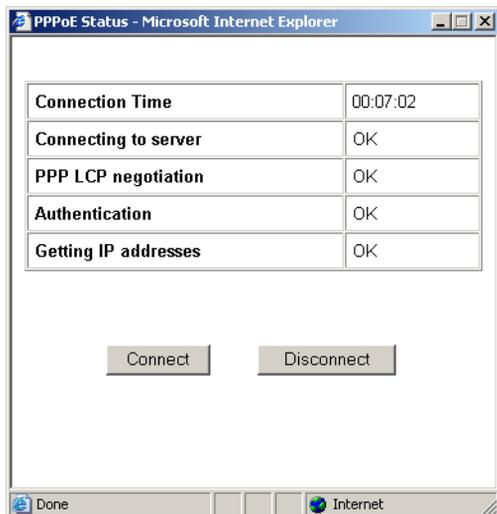

Figure 6-3.   PPPoE Status screen

The router will automatically authenticate with the PPPoE or PPPoA network when you have data to transmit. You can manually connect to the network by clicking on the Connect button.

This screen gives you more detailed information about your PPPoE or PPPoA link. When the connection is up and working, the amount of time that has elapsed since it came up is indicated in the Connection Time field. The Model DG814 gateway goes through the following steps to bring up a PPPoE or PPPoA connection.

1. The WAN LED indicates whether the ADSL physical layer can connect to the telephone companies ADSL equipment, called a DSL Access Multiplexor (DSLAM). The WAN LED will be solid green when this connection is made.

2. "Connecting to server", "PPP LCP negotiation" and "Authentication" indicate whether the router is able to reach the PPPoE or PPPoA server and authenticate the User Name and Password. If one of these steps fail it may indicate that the values entered in the WIZARD SETUP screens are not correct.

3. "Getting IP addresses" indicates whether the router has successfully received a DHCP assignment from the DHCP server. This step is not necessary if a static IP address has been assigned.

Click the "Ping Status" button to perform a connectivity test from your router, as shown in
Figure 6-4 below.
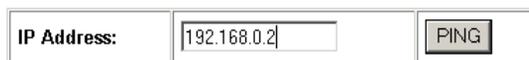
Figure 6-4.   Ping Status screen

This screen allows you to "ping" an IP address on the LAN to verify connectivity. Enter the IP
address and click the "PING" button to perform the test.

DHCP Table

The DHCP Table shows all IP address assignments that have been made by the gateway's DHCP
server. From the Main Menu of the browser interface, click Maintenance, then select DHCP Table
to view the table, shown in Figure 6-5, below.
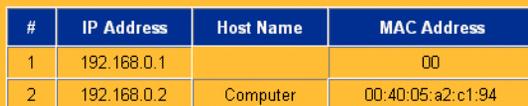
Figure 6-5.   DHCP Table

For each PC client, the table shows the IP address, NetBIOS Host Name and Ethernet MAC address. Note that if the gateway is rebooted, the table data is lost until each PC renews its DHCP lease.

Upgrade

The routing software of the Model DG814 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) file before sending it to the gateway. The upgrade file can be sent to the gateway using your browser.

Note: The Web browser used to upload new firmware into the Model DG814 gateway must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explore or Netscape Navigator 3.0 or above.

To reach the Upgrade menu, click Maintenance from the navigation bar on the left, and then click the UPGRADE heading. To upload new firmware:

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

2. In the Software Upgrade menu, click the Browse button and browse to the location of the binary (.BIN) upgrade file

3. Click Upload.

   Note: When uploading software to the Model DG814 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.

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

Configuration File Management

The configuration settings of the Model DG814 gateway are stored within the router in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

To manage the configuration file, click Maintenance in the Main Menu of the browser interface, then select Files. Three submenu tabs are available, and are described in the following sections.

Restore and Backup the Configuration

The Restore and Backup tabs in the Maintenance menu allow you to save and retrieve a file containing your gateway's configuration settings.

To save your settings, select the Backup tab. Click the Backup button. Your browser will extract the configuration file, named 'rom-0', from the gateway and will prompt you for a location on your PC to store the file.

To restore your settings, select the Restore tab. Enter the full path to the configuration file on your PC or click the Browse button to browse to the file. When you have located it, click the Upload button to send the file to the router. The router will then reboot automatically.

Erase the Configuration

It is sometimes desirable to restore the gateway to a known blank condition. This can be done by using the Erase function, which will restore all factory settings. After an erase, the router's password will be password, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

To erase the configuration, click the Erase tab, then click the Erase button on the screen.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See "Using the Default Reset button" on page 6-8.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the Manager 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 Manager (see "Erase the Configuration" on page 6-7).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the Manager password or IP address is not known.

Using the Default Reset button

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

1. Press the Default Reset button for 10 seconds, then release it.

   If the TEST LED begins to blink, the defaults have been restored and the router is now rebooting. Otherwise, go to step 2.

2. Disconnect the power from the router.

3. While depressing the Default Reset button, reconnect power to the router.

   Continue to hold the Default Reset button. The TEST LED will begin to blink, then will flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the router is now rebooting.

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

Chapter 7
Troubleshooting

This chapter gives information about troubleshooting your Model DG814 DSL Modem Internet Gateway. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

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

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

PWR LED Not On

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

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

•   Check that you are using the 18 V AC 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 Blinks or LED Stays On

When the router 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 router.

If you experience problems with the Test LED:

•   Cycle the power to see if the router 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 router recovers.

•   Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Using the Default Reset button" on page 6-8.

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

Troubleshooting the Web Configuration Interface

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

•   Check the Ethernet connection between your PC and the router as described in the previous section.

•   Make sure your PC's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to "Verifying TCP/IP Properties (Windows)" on page 3-5 or "Verifying TCP/IP Properties (Macintosh)" on page 3-8 to find your PC's IP address. Follow the instructions in Chapter 3 to configure your PC.

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

- If your router's IP address has been changed and you don't know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in "Using the Default Reset button" on page 6-8.

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

- Try quitting the browser and launching it again.

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

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

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes 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

ADSL link

If your router 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 you line correctly and that your wiring is correct.

WAN LED Blinking Yellow

If your WAN LED is blinking yellow then your router 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.

1. Temporarily connect a telephone to the ADSL line. This telephone will need to be removed and re-installed with a microfilter after your ADSL problem is debugged.

2. Listen for a dial tone. You should be able to hear a dial-tone on the ADSL line. If you cannot hear a dial tone then you are not connected to the ADSL signal. You may have the ADSL signal on the wrong pair of pins on you modular wall jack, in which case you will need to use a swapper, which is not provided. You also may have a problem will your household wiring.

3. If you have more than one telephone line, verify that you are connected to the correct one. From another telephone, call the phone number on which the telephone company installed ADSL. The temporary telephone should ring. If it does not, you are connected to the wrong line.

4. Disconnect the temporary telephone. You can reconnect it using a microfilter.

Obtaining a WAN IP Address

If your router is unable to access the internet, and your WAN LED is green or blinking green, you should determine whether the router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the 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 router'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 router has not obtained an IP address from your ISP.

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

• Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or 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 router in the browser-based Setup Wizard.

• Your ISP only allows one MAC address to connect to Internet, and may check for your PC's MAC address. In this case, inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

Troubleshooting PPPoE or PPPoA

The PPPoA or PPPoA connection can be debugged as follows:

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

2. Under the Maintenance heading, click the "Show PPPoE Status" or "Show PPPoA Status" button, depending on your connection type.

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 router 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 router will not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshooting Internet Browsing

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

• Your PC may not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your PC and verify the DNS address as described in "Verifying TCP/IP Properties (Windows)" on page 3-5. Alternatively, you may configure your PC manually with DNS addresses, as explained in your operating system documentation.

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

If your PC obtains its information from the router by DHCP, reboot the PC and verify the gateway address as described in "Verifying TCP/IP Properties (Windows)" on page 3-5.

Troubleshooting a TCP/IP Network Using a Ping Utility

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

Testing the LAN Path to 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 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 OK.

   You should see a message like this one:

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

   If the path is working, you see this message:

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

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

   `Request timed out`

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

   • Wrong physical connections

     — Make sure the LAN LNK/ACT LED is on. If the LNK/ACT LED is off, follow the instructions in "Troubleshooting the Web Configuration Interface" 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. Go to the Run… window and run winipcfg. Verify that the IP address of the router is listed as the default gateway as described in"Verifying TCP/IP Properties" on page 3-6.

— 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.

— If your ISP assigned a host name to your PC, enter that host name as the router name in the Wizard Setup.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The Model DG814 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 Model DG814 DSL Modem Internet Gateway.

General Specifications

Network Protocol and Standards Compatibility

Data and Routing Protocols:	TCP/IP
	RIP-1/RIP-2
	DHCP server and DHCP relay
	RFC 1483, 2684 Bridged Ethernet Encapsulation
	RFC 2516 PPP over Ethernet (PPPoE)
	RFC 2364 PPP over ATM (PPPoA)
	RFC 1577 Classical IP over ATM

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):	18 V AC @ 0.4A output, 30W maximum

Physical Specifications

Dimensions:	255 by 169 by 34 mm 10.0 by 6.7 by 1.3 in.
Weight:	0.54 kg 1.2 lb.

Environmental Specifications

Operating temperature:	0° to 40° C
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 A

Appendix B
Networks and Routing Basics

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

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 Model DG814 DSL Modem Internet Gateway is a residential or small office router that routes the IP protocol over a single-user ADSL 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 Model DG814 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.
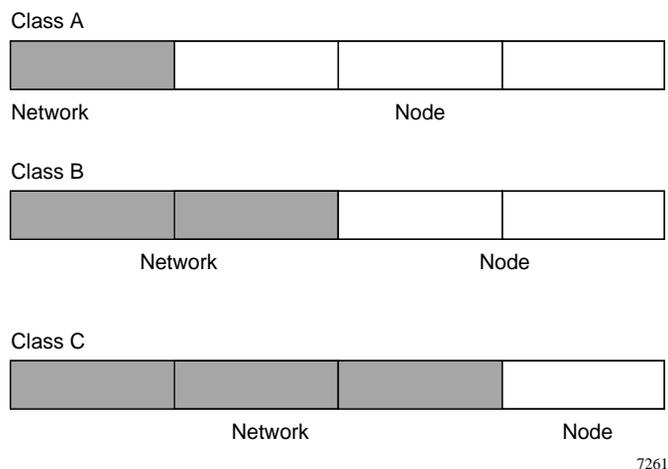
Class A

Network   Node

Class B

Network   Node

Class C

Network   Node

7261

Figure B-1.   Three Main Address Classes

The five address classes are:

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

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

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

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

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

  `192.0.1.x to 223.255.254.x.`

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

  `224.0.0.0 to 239.255.255.255.`

- Class E
  Class E addresses are for experimental use.

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

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

Netmask

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

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

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

combined with:

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

Equals:

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

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

Subnet Addressing

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

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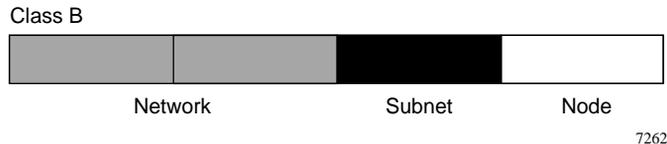
Class B

Network		Subnet	Node

7262

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

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

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

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

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

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

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

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

Table B-2.   Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
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 Model DG814 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 Model DG814 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.
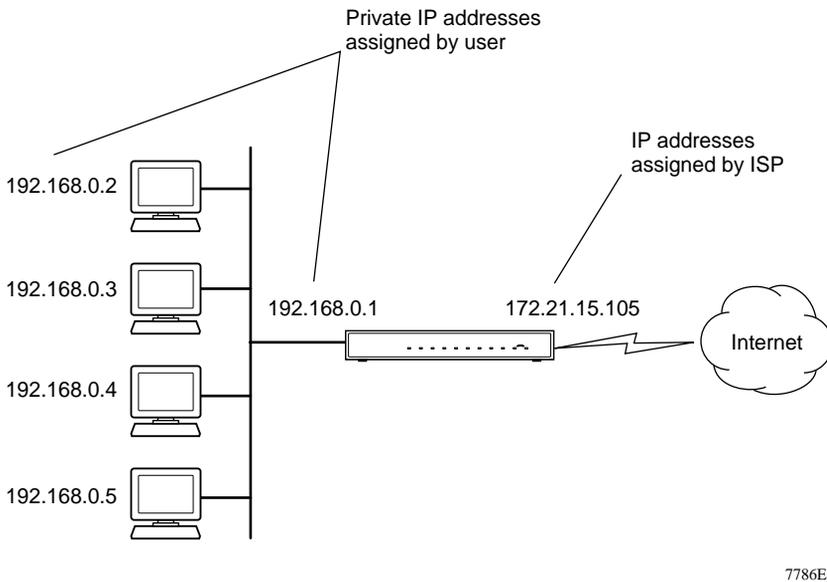
Figure B-3.   Single IP Address Operation Using NAT

This scheme offers the additional benefit of simple 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.

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.

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 Model DG814 gateway has the capacity to act as a DHCP server.

The Model DG814 gateway also functions as a DHCP client when connecting to the ISP. The router 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 and pinout as described in Table B-3.

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

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

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependent Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependent Interface - Crossover (MDI-X). When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of three mechanisms:

• Uplink switch
  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.

- Crossover cable
  A crossover cable 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.

- Auto MDI/MDI-X switching
  Some Ethernet switch products, such as the Model DG814 gateway, are able to sense the polarity of a connection and automatically adapt to the proper mating polarity.

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.

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.
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	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.
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.
IPX	*See* Internet Packet Exchange.
ISP	Internet service provider.
Internet Packet Exchange	Novell's internetworking protocol.
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.
MSB	*See* Most Significant Bit or Most Significant Byte.
MRU	*See* Maximum Receive Unit.
Maximum Receive 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.
NID	Network Interface Device. The point of demarcation, where the telephone line comes into the house.
Packet	A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.
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.
VPN	Virtual Private Network. A method for securely transporting data between two private networks by using a public network such as the Internet as a connection.
WAN	*See* wide area network.
Wide Area Network	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
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