

Reference Manual for the Mobile Broadband Router MBR814X



NETGEAR

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

202-10005-05
June 2005

© 2005 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR is a trademark of Netgear, Inc.

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

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

Statement of Conditions

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

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

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

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

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

Federal Communications Commission (FCC) Radiation Exposure Statement

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

EN 55 022 Declaration of Conformance

This is to certify that the 54 Mbps Mobile Broadband Router MBR814 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 54 Mbps Mobile Broadband Router MBR814 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 54 Mbps Mobile Broadband Router MBR814 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 54 Mbps Mobile Broadband Router MBR814.

World Wide Web

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

Product and Publication Details

Model Number:	MBR814X
Publication Date:	June 2005
Product Family:	router
Product Name:	54 Mbps Mobile Broadband Router MBR814X
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10005-05

Regulatory Approvals

FCC Statement

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 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.

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons.

Channel

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple Access Points, it is better if adjacent Access Points use different Channels to reduce interference.
- In "Infrastructure" mode, Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If using "Ad-hoc" mode (no Access Point), all Wireless stations should be set to use the same Channel. However, most Wireless stations will still scan all Channels to see if there is an existing "Ad-hoc" group they can join.

About the PCMCIA Wireless Network Card,

The slot of the device Mobile Broadband Router will only accept and can only collocate with this PCMCIA Wireless Network Card, model: FPC-1000 (FCC ID: QZX99171001) manufactured by FLARION TECHNOLOGIES, INC., and may not be collocated with any other radio cards

Contents

Chapter 1

About This Manual

Audience, Scope, Conventions, and Formats	1-1
How to Use This Manual	1-2
How to Print this Manual	1-2

Chapter 2

Introduction

About the Router	2-1
Key Features	2-1
802.11 Standards-based Wireless Networking	2-2
A Powerful, True Firewall	2-2
Content Filtering	2-3
Auto Sensing and Auto Uplink™ LAN Ethernet Connections	2-3
Protocol Support	2-3
Easy Installation and Management	2-4
What's in the Box?	2-5
The Router's Front Panel	2-5
The Router's Rear Panel	2-6

Chapter 3

Connecting the Router to the Internet

Ethernet Cabling Requirements	3-1
Computer Hardware Requirements	3-1
LAN Configuration Requirements	3-1
Internet Configuration Requirements	3-2
Where Do I Get the Internet Configuration Parameters?	3-2
Record Your Internet Connection Information	3-3
Connecting the MBR814 to Your LAN	3-4
First, install the router.	3-4
Next, log in to the router.	3-5

Then, connect to the Internet.	3-6
Testing Your Internet Connection	3-7
Manually Configuring Your Internet Connection	3-7

Chapter 4

Wireless Configuration

Considerations for a Wireless Network	4-1
Observe Performance, Placement, and Range Guidelines	4-1
Implement Appropriate Wireless Security	4-2
Understanding Wireless Settings	4-3
How to Set Up and Test Basic Wireless Connectivity	4-7
How to Restricting Wireless Access to Your Network	4-8
Restricting Access to Your Network by Turning Off Wireless Connectivity	4-9
Restricting Wireless Access Based on the Wireless Network Name (SSID)	4-9
Restricting Wireless Access Based on the Wireless Station Access List	4-9
Choosing WEP Authentication and Security Encryption Methods	4-11
Authentication Type Selection	4-11
Encryption Choices	4-12
How to Configure WEP	4-13
How to Configure WPA-PSK	4-14

Chapter 5

Protecting Your Network

Protecting Access to Your 54Mbps Mobile Broadband Router MBR814	5-1
How to Change the Built-In Password	5-1
Changing the Administrator Login Timeout	5-2
Configuring Basic Firewall Services	5-2
Blocking Keywords, Sites, and Services	5-3
How to Block Keywords and Sites	5-3
Firewall Rules	5-5
Inbound Rules (Port Forwarding)	5-6
Inbound Rule Example: A Local Public Web Server	5-7
Inbound Rule Example: Allowing Videoconferencing	5-8
Considerations for Inbound Rules	5-9
Outbound Rules (Service Blocking)	5-9
Outbound Rule Example: Blocking Instant Messenger	5-9
Order of Precedence for Rules	5-11

Services	5-12
How to Define Services	5-12
Setting Times and Scheduling Firewall Services	5-13
How to Set Your Time Zone	5-13
How to Schedule Firewall Services	5-14

Chapter 6

Managing Your Network

Backing Up, Restoring, or Erasing Your Settings	6-1
How to Back Up the Configuration to a File	6-1
How to Restore the Configuration from a File	6-2
How to Erase the Configuration	6-2
Upgrading the Router's Firmware	6-2
How to Upgrade the Router Firmware	6-3
Network Management Information	6-3
Viewing Router Status and Usage Statistics	6-4
Viewing Attached Devices	6-8
Viewing, Selecting, and Saving Logged Information	6-8
Selecting What Information to Log	6-10
Saving Log Files on a Server	6-11
Examples of Log Messages	6-11
Activation and Administration	6-11
Dropped Packets	6-11
Enabling Security Event E-mail Notification	6-12
Running Diagnostic Utilities and Rebooting the Router	6-13
Enabling Remote Management	6-14
Configuring Remote Management	6-14

Chapter 7

Advanced Configuration

Configuring Advanced Security	7-1
Setting Up A Default DMZ Server	7-1
How to Configure a Default DMZ Server	7-2
Connect Automatically, as Required	7-3
Disable Port Scan and DOS Protection	7-3
Respond to Ping on Internet WAN Port	7-3
MTU Size	7-3

Configuring LAN IP Settings	7-3
DHCP	7-5
Use Router as DHCP server	7-5
Reserved IP addresses	7-6
How to Configure LAN TCP/IP Settings	7-6
Configuring Dynamic DNS	7-7
How to Configure Dynamic DNS	7-8
Using Static Routes	7-9
Static Route Example	7-9
How to Configure Static Routes	7-10
Universal Plug and Play (UPnP)	7-11
Chapter 8	
Troubleshooting	
Basic Functioning	8-1
Power LED Not On	8-2
Test LED Never Turns On or Test LED Stays On	8-2
LAN or WAN Port LEDs Not On	8-2
Troubleshooting the Web Configuration Interface	8-3
Troubleshooting the ISP Connection	8-4
ADSL link	8-4
Internet LED Off	8-4
Obtaining an Internet IP Address	8-4
Troubleshooting Internet Browsing	8-5
Troubleshooting a TCP/IP Network Using the Ping Utility	8-5
Testing the LAN Path to Your Router	8-6
Testing the Path from Your Computer to a Remote Device	8-6
Restoring the Default Configuration and Password	8-7
Using the Reset button	8-7
Problems with Date and Time	8-8
Appendix A	
Technical Specifications	A1
Appendix B	
Network and Routing Basics	
Related Publications	B-1
Basic Router Concepts	B-1

What is a Router?	B-1
Routing Information Protocol	B-2
IP Addresses and the Internet	B-2
Netmask	B-4
Subnet Addressing	B-4
Private IP Addresses	B-7
Single IP Address Operation Using NAT	B-7
MAC Addresses and Address Resolution Protocol	B-8
Related Documents	B-9
Domain Name Server	B-9
IP Configuration by DHCP	B-9
Internet Security and Firewalls	B-10
What is a Firewall?	B-10
Stateful Packet Inspection	B-10
Denial of Service Attack	B-11
Ethernet Cabling	B-11
Category 5 Cable Quality	B-11
Inside Twisted Pair Cables	B-12
Uplink Switches, Crossover Cables, and MDI/MDIX Switching	B-13

Appendix C

Preparing Your Network

Preparing Your Computers for TCP/IP Networking	C-1
Configuring Windows 95, 98, and Me for TCP/IP Networking	C-2
Installing or Verifying Windows Networking Components	C-2
Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 95B, 98, and Me C-4	
Selecting the Windows' Internet Access Method	C-6
Verifying TCP/IP Properties	C-6
Configuring Windows NT4, 2000 or XP for IP Networking	C-7
Installing or Verifying Windows Networking Components	C-7
DHCP Configuration of TCP/IP in Windows XP, 2000, or NT4	C-8
DHCP Configuration of TCP/IP in Windows XP	C-8
DHCP Configuration of TCP/IP in Windows 2000	C-10
DHCP Configuration of TCP/IP in Windows NT4	C-13
Verifying TCP/IP Properties for Windows XP, 2000, and NT4	C-15
Configuring the Macintosh for TCP/IP Networking	C-16

MacOS 8.6 or 9.x	C-16
MacOS X	C-16
Verifying TCP/IP Properties for Macintosh Computers	C-17
Verifying the Readiness of Your Internet Account	C-18
Are Login Protocols Used?	C-18
What Is Your Configuration Information?	C-18
Obtaining ISP Configuration Information for Windows Computers	C-19
Obtaining ISP Configuration Information for Macintosh Computers	C-20
Restarting the Network	C-21

Appendix D

Wireless Networking Basics

Wireless Networking Overview	D-1
Infrastructure Mode	D-1
Ad Hoc Mode (Peer-to-Peer Workgroup)	D-2
Network Name: Extended Service Set Identification (ESSID)	D-2
Authentication and WEP Data Encryption	D-2
802.11 Authentication	D-3
Open System Authentication	D-3
Shared Key Authentication	D-4
Overview of WEP Parameters	D-5
Key Size	D-6
WEP Configuration Options	D-7
Wireless Channels	D-7
WPA Wireless Security	D-8
How Does WPA Compare to WEP?	D-9
How Does WPA Compare to IEEE 802.11i?	D-10
What are the Key Features of WPA Security?	D-10
WPA Authentication: Enterprise-level User Authentication via 802.1x/EAP and RADIUS	D-12
WPA Data Encryption Key Management	D-14
Is WPA Perfect?	D-16
Product Support for WPA	D-16
Supporting a Mixture of WPA and WEP Wireless Clients is Discouraged	D-16
Changes to Wireless Access Points	D-16
Changes to Wireless Network Adapters	D-17
Changes to Wireless Client Programs	D-18

Appendix E

Virtual Private Networking

What is a VPN?	E-1
What Is IPSec and How Does It Work?	E-2
IPSec Security Features	E-2
IPSec Components	E-2
Encapsulating Security Payload (ESP)	E-3
Authentication Header (AH)	E-4
IKE Security Association	E-4
Mode	E-5
Key Management	E-6
Understand the Process Before You Begin	E-6
VPN Process Overview	E-7
Network Interfaces and Addresses	E-7
Interface Addressing	E-7
Firewalls	E-8
Setting Up a VPN Tunnel Between Gateways	E-8
VPNC IKE Security Parameters	E-10
VPNC IKE Phase I Parameters	E-10
VPNC IKE Phase II Parameters	E-11
Testing and Troubleshooting	E-11
Additional Reading	E-11

Appendix F

NETGEAR VPN Configuration

MBR814 to FVL328	F-1
Configuration Profile	F-1
Step-By-Step Configuration	F-2
MBR814 with FQDN to FVL328	F-6
Configuration Profile	F-6
The Use of a Fully Qualified Domain Name (FQDN)	F-7
Step-By-Step Configuration	F-8
Configuration Summary (Telecommuter Example)	F-13
Setting Up the Client-to-Gateway VPN Configuration (Telecommuter Example)	F-14
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the VPN Router at the Employer's Main Office	F-14

Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC at the Telecommuter's Home Office	F-16
Monitoring the VPN Tunnel (Telecommuter Example)	F-25
Viewing the PC Client's Connection Monitor and Log Viewer	F-25
Viewing the VPN Router's VPN Status and Log Information	F-27
Glossary	

Chapter 1

About This Manual

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

Audience, Scope, Conventions, and Formats

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

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

<i>italics</i>	Emphasis, books, CDs, URL names
bold	User input
<code>fixed</code>	Screen text, file and server names, extensions, commands, IP addresses

This guide uses the following formats to highlight special messages:

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

This manual is written for the MBR814 router according to these specifications:

Table 1-2. Manual Scope

<i>Product Version</i>	54 Mbps Mobile Broadband Router MBR814
Manual Publication Date	June 2005

	Note: Product updates are available on the NETGEAR, Inc. Web site at http://kbserver.netgear.com/products/MBR814.asp .
---	---

How to Use This Manual

The HTML version of this manual includes the following:

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

How to Print this Manual

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

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

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

- **Printing a Chapter.**

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

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

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

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

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

- **Printing the Full Manual.**

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

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

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

Chapter 2

Introduction

This chapter describes the features of the NETGEAR 54 Mbps Mobile Broadband Router MBR814. The MBR814 router is a combination of a wireless broadband modem, router, 4-port switch, and firewall which enables your entire network to safely share an Internet connection.



Note: If you are unfamiliar with networking and routing, refer to [Appendix B, “Network and Routing Basics”](#) to become more familiar with the terms and procedures used in this manual.

About the Router

The 54 Mbps Mobile Broadband Router MBR814 provides continuous, high-speed 10/100 Ethernet access between your Ethernet devices. The MBR814 router enables your entire network to share an Internet connection through the wireless broadband modem that otherwise is used by a single computer. With minimum setup, you can install and use the router within minutes.

The MBR814 router provides multiple Web content filtering options, plus e-mail browsing activity, reporting, and instant alerts. Parents and network administrators can establish restricted access policies based on time of day, Web site addresses, and address keywords. They can also share high-speed Internet access for up to 253 personal computers. The included firewall and Network Address Translation (NAT) features protect you from hackers.

Key Features

The MBR814 router provides the following features:

- A powerful, true firewall.
- 802.11g standards-based wireless networking.
- Content filtering.
- Auto Sensing and Auto Uplink™ LAN Ethernet connections.

- Easy, Web-based setup for installation and management.
- Extensive Internet protocol support.
- A card slot with PC card for wireless broadband access.

These features are discussed below.

802.11 Standards-based Wireless Networking

The MBR814 router includes an 802.11 g-compliant wireless access point, providing continuous, high-speed 10/100 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11 g Standards-based wireless networking at up to 100 Mbps.
- Works with both 802.11g and 802.11b wireless devices.
- 64-bit and 128-bit WEP encryption security.
- WEP keys can be entered manually or generated by passphrase.
- Support for the Wi-Fi Protected Pre-Shared Key (WPA-PSK) encryption and 802.1x authentication.
- Wireless access can be restricted by MAC address.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the MBR814 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection
Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents
The MBR814 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to email the log to you at specified intervals. You can also configure the router to send immediate alert messages to your email address or email pager whenever a significant event occurs.

Content Filtering

With its content filtering feature, the MBR814 prevents objectionable content from reaching your computers. The router allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the router to log and report attempts to access objectionable Internet sites.

Auto Sensing and Auto Uplink™ LAN Ethernet Connections

With its internal 4-port 10/100 switch, the MBR814 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The local LAN ports are autosensing and capable of full-duplex or half-duplex operation.

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

Protocol Support

The MBR814 supports Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). [Appendix B, “Network and Routing Basics”](#) provides further information on TCP/IP.

- **The Ability to Enable or Disable IP Address Sharing by NAT**
The MBR814 allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account. This feature can also be turned off completely while using the MBR814 if you want to manage the IP address scheme yourself.
- **Automatic Configuration of Attached PCs by DHCP**
The MBR814 dynamically assigns network configuration information, including IP, router, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- **DNS Proxy**
When DHCP is enabled and no DNS addresses are specified, the router provides its own address as a DNS server to the attached PCs. The router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.

- **Classical IP (RFC 1577)**
Some Internet service providers, in Europe for example, use Classical IP in their ADSL services. In such cases, the router is able to use the Classical IP address from the ISP.
- **Dynamic DNS**
Dynamic DNS services allow remote users to find your network using a domain name when your IP address is not permanently assigned. The router contains a client that can connect to many popular Dynamic DNS services to register your dynamic IP address.
- **Universal Plug and Play (UPnP)**
UPnP is a networking architecture that provides compatibility between networking technologies. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

Easy Installation and Management

You can install, configure, and operate the MBR814 within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**
Browser-based configuration allows you to easily configure your router from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **Remote management**
The router allows you to log in to the Web management interface from a remote location via the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.
- **Diagnostic functions**
The router incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the router. You can use these diagnostic functions directly from the MBR814 when you are connected on the LAN or when you are connected over the Internet via the remote management function.
- **Visual monitoring**
The router's front panel LEDs provide an easy way to monitor its status and activity.
- **Flash erasable programmable read-only memory (EPROM) for firmware upgrades.**

What's in the Box?

The product package should contain the following items:

- 54 Mbps Mobile Broadband Router MBR814
- AC power adapter (varies by region)
- Category 5 (Cat 5) Ethernet cable
- *Resource CD*, including:
 - This guide
 - Application Notes
- A Printed Quick Installation Guide
- Warranty and Support Information Cards

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

The Router's Front Panel

The 54 Mbps Mobile Broadband Router MBR814 front panel shown below contains status LEDs.

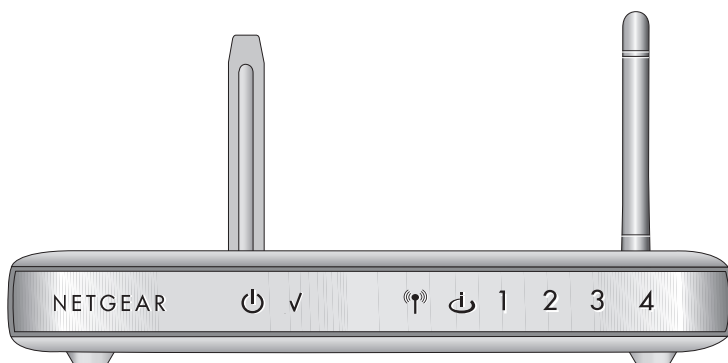


Figure 2-1: MBR814 Front Panel

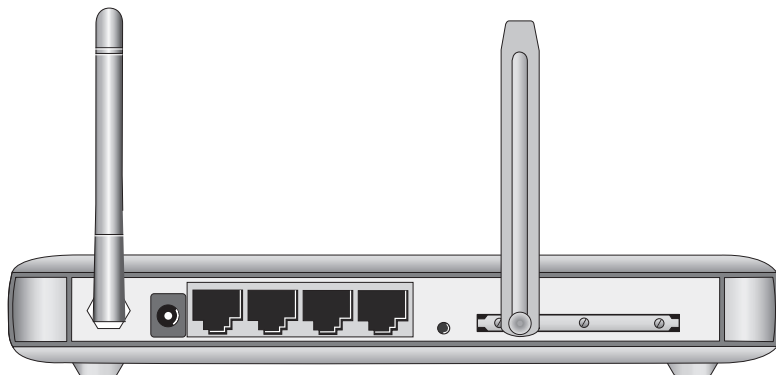
You can use the LEDs to verify various conditions. [Table 2-1](#) lists and describes each LED on the front panel of the router. These LEDs are green when lit.

Table 2-1. LED Descriptions

LED	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.
Wireless 	On Off	Indicates that the Wireless port is initialized. The Wireless Access Point is turned off.
Internet 	On — Green Blink — Green	The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
LAN 	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The Local port has detected a link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected a 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 54 Mbps Mobile Broadband Router MBR814 contains port connections.

**Figure 2-2: MBR814 Rear Panel**

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

- Wireless antenna
- AC power adapter outlet
- Four Local Ethernet RJ-45 ports for connecting the router to the local computers
- Factory Default Reset push button
- Slot with wireless broadband PC Card

Chapter 3

Connecting the Router to the Internet

This chapter describes how to set up the router on your Local Area Network (LAN) and connect to the Internet. It describes how to configure your Mobile Broadband Router MBR814 for Internet access.

Minimum Requirements

The MBR814 is designed for easy installation. Make sure that these minimum requirements are met.

- You must have an account for wireless broadband service, and you must be located in an area with wireless broadband coverage. Check with your Internet service provider if you are not sure.
- Observe the guidelines for placement of wireless equipment as described in the *CROSS REF HERE*.
- Your computer must have a wireless adapter or wireless card that is set up to run on your network; and it must be configured with DHCP.

Ethernet Cabling Requirements

The MBR814 router connects to your Ethernet LAN via twisted-pair cables. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your router.

Computer Hardware Requirements

To use the MBR814 router on your network, each computer must have an installed Ethernet adapter and an Ethernet cable, or a 802.11g wireless adapter.

LAN Configuration Requirements

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

Note: Please refer to [Appendix C, “Preparing Your Network”](#) for assistance with DHCP configuration.

Internet Configuration Requirements

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

- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses
- Fixed or Static IP Address

Where Do I Get the Internet Configuration Parameters?

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

- Your ISP should have provided you with all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
 - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties.
 - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties.
 - For Macintosh computers, open the TCP/IP or Network control panel.
- You can also refer to the *MBR814 Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

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

Record Your Internet Connection Information

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

ISP Multiplexing Method and Virtual Circuit Number: The default settings of your Mobile Broadband Router MBR814 will work fine for most ISPs.

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

Login Name: _____ Password: _____

Service Name: _____

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

Fixed or Static Internet IP Address: _____

Router IP Address: _____

Subnet Mask: _____

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

Primary DNS Server IP Address: _____

Secondary DNS Server IP Address: _____

Host and Domain Names: Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you did not get host or domain names, use the following examples as a guide:

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

ISP Host Name: _____ ISP Domain Name: _____

Connecting the MBR814 to Your LAN

This section provides instructions for connecting the MBR814 router.

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

There are three steps to connecting your router:

1. Install the router.
2. Log in to the router.
3. Connect to the Internet.

Note: Follow the steps below to connect your router to your network. Before you begin, locate the configuration information from your Internet Service Provider (ISP).

First, install the router.

1. Turn off your computer.
2. Check the router to make sure that the broadband card is securely inserted in the slot in the back of the router. Please refer to the applicable sections in the appendix or the user manual provided with the broadband card for additional installation information.
3. Connect the Ethernet cable that came with your router into a LAN port on the router such as LAN port 4, and then connect the other end into the Ethernet port of your computer.

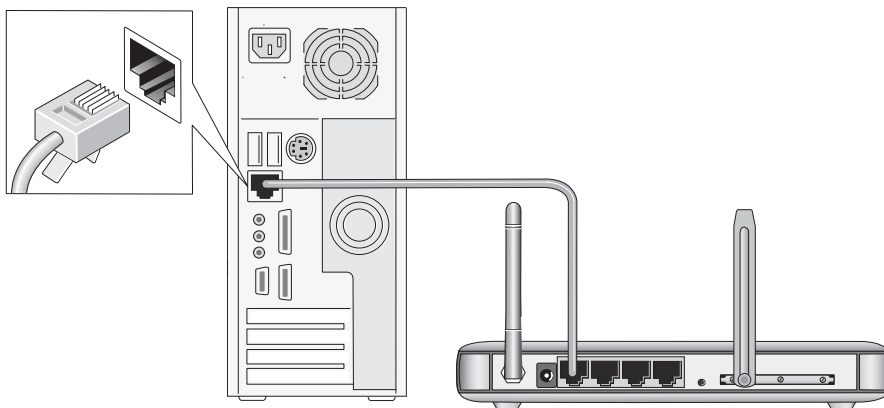


Figure 3-1: Connect the router to your computer

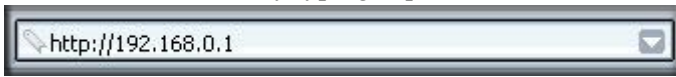
4. Plug in the power adapter to your router. Verify the following:
 -  The power light is lit after applying power to the router.
 -  The Status light comes on briefly and then goes off.

Note: If applicable, the status light on the broadband card shows that it is active. Please refer to the broadband card user manual for details.

Next, log in to the router.

Note: Your computer needs to be configured for DHCP. For instructions on configuring for DHCP, please see [Appendix C, “Preparing Your Network”](#).

1. Turn on your computer, let the operating system boot up completely, and log in as needed.
2. The light on the router for the port connected to the computer lights up.
3. From the Ethernet connected computer you just set up, open a browser such as Internet Explorer or Netscape® Navigator.
4. Connect to the router by typing *http://192.168.0.1* in the address field of your browser.



A login window opens as shown below:

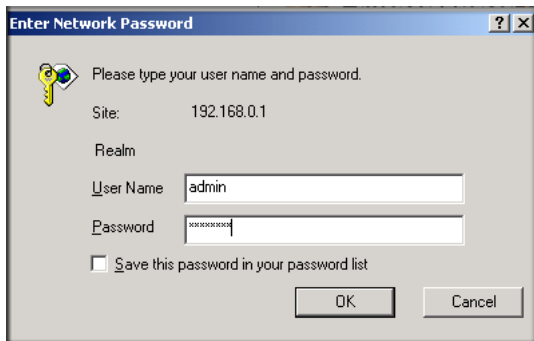


Figure 3-2: Login window

- a. Enter **admin** for the user name and **password** for the password, both in lower case letters. After logging in you will see the Basic Setup menu.

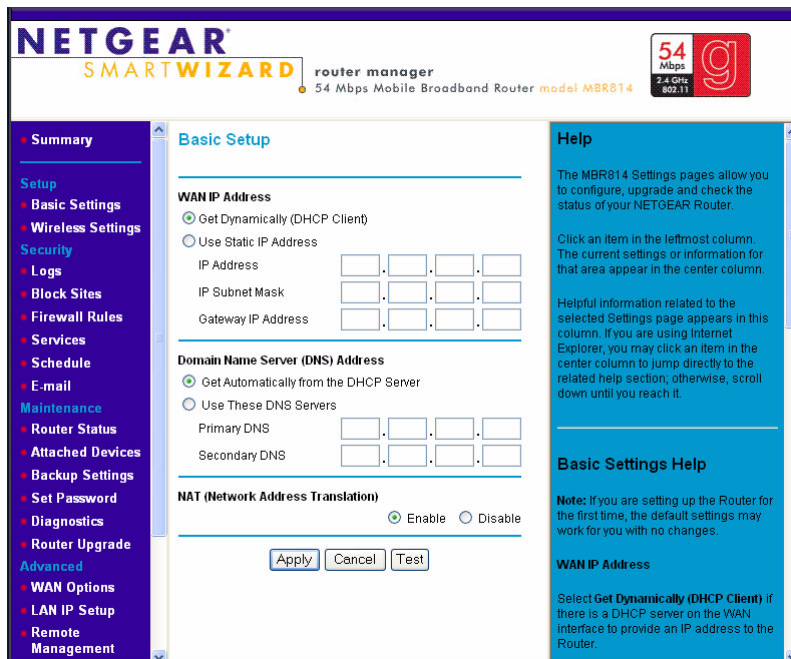


Figure 3-3: Basic Settings menu

Then, connect to the Internet.

1. Check the Router Status page to make sure that wireless broadband coverage is available.
2. Verify connectivity to the Internet by opening a browser or verify access to network resources such as files and printers.
3. Make any needed configuration changes to fit your wireless local area network (WLAN) such as setting up wireless security.

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

Unless your ISP automatically assigns your configuration automatically via DHCP, you need the configuration parameters from your ISP you recorded in [“Record Your Internet Connection Information”](#) on page 3-3.

Testing Your Internet Connection

After completing the Internet connection configuration, you can test your Internet connection. Log in to the router, then, from the Basic Settings link in the Setup menu, click the Test button. If the NETGEAR Web site does not appear within one minute, refer to [Chapter 8](#), “Troubleshooting”.

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

To access the Internet from any computer 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.

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

Manually Configuring Your Internet Connection

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

1. Set the WAN IP Address:

- Select “Get Dynamically from ISP” if your ISP uses DHCP to assign your IP address. Your ISP will automatically assign these addresses.
- Select “Use Static IP Address” if your ISP has assigned you a permanent, fixed (static) IP address. Enter the IP address that your ISP assigned. Also enter the IP Subnet Mask and the Gateway IP Address. The gateway is the ISP’s router to which your router will connect.

The screenshot shows the 'Basic Setup' configuration page. It is divided into three main sections: WAN IP Address, Domain Name Server (DNS) Address, and NAT (Network Address Translation). In the WAN IP Address section, 'Get Dynamically (DHCP Client)' is selected. In the DNS section, 'Get Automatically from the DHCP Server' is selected. In the NAT section, 'Enable' is selected. At the bottom, there are 'Apply', 'Cancel', and 'Test' buttons.

Basic Setup			
WAN IP Address			
☒ Get Dynamically (DHCP Client)			
☐ Use Static IP Address			
IP Address			
IP Subnet Mask			
Gateway IP Address			
Domain Name Server (DNS) Address			
☒ Get Automatically from the DHCP Server			
☐ Use These DNS Servers			
Primary DNS			
Secondary DNS			
NAT (Network Address Translation)			
☒ Enable ☐ Disable			
Apply Cancel Test			

2. Specify the Domain Name Server (DNS) Address:

- Select “Get Dynamically from ISP” if your ISP uses DHCP to assign your IP address. Your ISP will automatically assign this address.
- If you know that your ISP does not automatically transmit DNS addresses to the router during login, select “Use these DNS servers” and enter the IP address of your ISP’s Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

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

3. You should only disable NAT if you are sure you do not require it. NAT automatically assigns private IP addresses (192.168.0.x) to LAN connected devices. When NAT is disabled, only standard routing is performed by this router.

Classical routing lets you directly manage the IP addresses the MBR814 uses. Classical routing should be selected only by experienced users.

Note: Disabling NAT will reboot the router and reset all the MBR814 configuration settings to the factory default. Disable NAT only if you plan to install the MBR814 in a setting where you will be manually administering the IP address space on the LAN side of the router

4. Router MAC Address:

This section determines the Ethernet MAC address that will be used by the router on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your computer when your account is first opened. They will then only accept traffic from the MAC address of that computer. This feature allows your router to masquerade as that computer by “cloning” its MAC address.

To change the MAC address, select “Use this Computer’s MAC address”. The router will then capture and use the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP. Alternatively, select “Use this MAC address” and enter it.

5. Click **Apply** to save your settings.
6. Click the Test button to test your Internet connection.

If the NETGEAR Web site does not appear within one minute, refer to [Chapter 8](#), “Troubleshooting”.

Chapter 4

Wireless Configuration

This chapter describes how to configure the wireless features of your 54 Mbps Mobile Broadband Router MBR814.

Considerations for a Wireless Network

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your router in order to maximize the network speed. For further information, refer to [Appendix D, “Wireless Networking Basics”](#).

Observe Performance, Placement, and Range Guidelines

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



Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router. For complete range/performance specifications, please see [Appendix A, “Technical Specifications”](#).

For best results, place your firewall:

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

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

Implement Appropriate Wireless Security



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

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The MBR814 router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

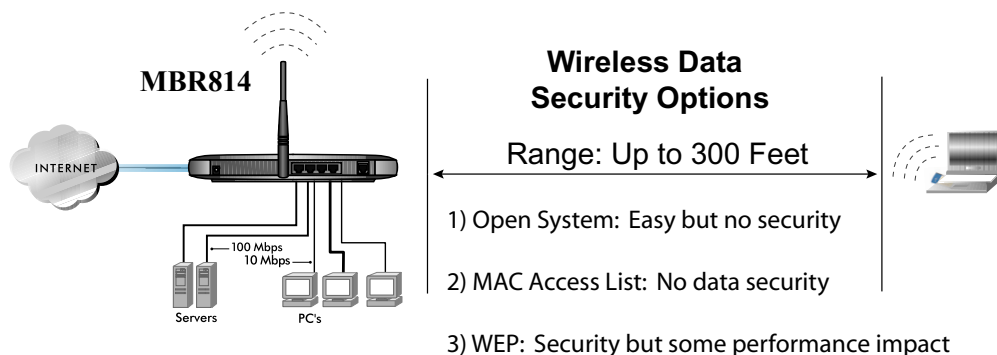


Figure 4-1: MBR814 wireless data security options

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

- **Restrict Access Based on MAC Address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the MBR814. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network ‘discovery’ feature of some products, such as Windows XP, but the data is still exposed.

- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.
- **WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame re-keying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.

Understanding Wireless Settings

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

Mode: g & b

Wireless Access Point

☒ Enable Wireless Access Point

☒ Allow Broadcast of Name (SSID)

☐ Wireless Isolation

Wireless Station Access List Setup Access List

Security Options

☐ Disable

☒ WEP (Wired Equivalent Privacy)

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

☐ WPA-802.1x

WEP Security Encryption

Authentication Type: Automatic

Encryption Strength: 64 bit

WEP Key

Passphrase: Generate

Key 1: ☒

Key 2: ☐

Key 3: ☐

Key 4: ☐

Apply Cancel

Figure 4-2: Wireless Settings menu

The following parameters are in the Wireless Settings menu:

- **Wireless Network.**

- **Name (SSID).** The Service Set ID, also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is **NETGEAR**, but NETGEAR strongly recommends that you change your network Name to a different value.

Note: This value is case sensitive. For example, **Wireless** is not the same as **wireless**.

— **Region.** The region can not be changed by users

— **Mode.** The default is "g & b", which allows both "g" and "b" wireless stations to access this device. "g only" allows only 802.11g wireless stations to be used. "b only" allows 802.11b wireless stations; 802.11g wireless stations can still be used if they can operate in 802.11b mode.

- **Wireless Access Point.**

— **Enable Wireless Access Point.** This field lets you turn off or turn on the wireless access point built in to the router. The wireless icon on the front of the router will also display the current status of the Wireless Access Point to let you know if it is disabled or enabled. The wireless access point must be enabled to allow wireless stations to access the Internet.

— **Allow Broadcast of Name (SSID).** If enabled, the SSID is broadcast to all Wireless Stations. Stations which have no SSID (or a "null" value) can then adopt the correct SSID for connections to this Access Point.

— **Wireless Isolation.** If enabled, Wireless Stations will not be able to communicate with each other or with Stations on the wired network. This feature should normally be disabled.

- **Wireless Station Access List.**

— By default, any wireless computer that is configured with the correct wireless network name or SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only specific computers based on their MAC addresses. Click Setup Access List to display the Wireless Station Access List menu.

- Security Options

Table 4-1. Wireless Security Options

Field	Description
Disable	Wireless security is not used.
WEP (Wired Equivalent Privacy)	You can select the following WEP options: Authentication Type • Open: the MBR814 does not perform any authentication. • Shared: WEP shared key authentication. For a full explanation of WEP shared key, see “Authentication and WEP Data Encryption” on page D-2. Encryption Strength • If Shared or Open Network Authentication is enabled, you can choose 64- or 128-bit WEP data encryption. Note: With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the MBR814 <i>does</i> perform 64- or 128-bit data encryption but <i>does not</i> perform any authentication. Security Encryption (WEP) Key These key values must be identical on all wireless devices in your network (key 1 must be the same for all, key 2 must be the same for all, and so on). The MBR814 provides two methods for creating WEP encryption keys: • Passphrase. These characters <i>are</i> case sensitive. Enter a word or group of printable characters in the Passphrase box and click the Generate button. Note: Not all wireless adapters support passphrase key generation. • Manual. These values <i>are not</i> case sensitive. 64-bit WEP: enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F). 128-bit WEP: enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

Table 4-1. Wireless Security Options

Field	Description
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	WPA Pre-Shared-Key uses a pre-shared key to perform the authentication and generate the initial data encryption keys. Then, it dynamically varies the encryption key. For a full explanation of WPA, see “WPA Wireless Security” on page D-8. Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.
WPA-802.1x	User authentication is implemented using 802.1x and RADIUS servers. For a full explanation of WPA, see “WPA Wireless Security” on page D-8. Fill in the following: • Radius Server Name/IP Address This field is required. Enter the name or IP address of the Radius Server on your LAN. • Radius Port Enter the port number used for connections to the Radius Server. • Radius Shared Key Enter the desired value for the Radius shared key. This key enables the MBR814 to log in to the Radius server and must match the value used on the Radius server.

How to Set Up and Test Basic Wireless Connectivity

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

1. Log in to the MBR814 firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless Settings link in the main menu of the MBR814 firewall.
3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is **Wireless**.

Note: The SSID of any wireless access adapters must match the SSID you configure in the 54 Mbps Mobile Broadband Router MBR814. If they do not match, you will not get a wireless connection to the MBR814.

6. For initial configuration and test, leave the Wireless Card Access List set to allow everyone access by making sure that “Turn Access Control On” is not selected in the Wireless Station Access List. In addition, leave the Encryption Strength set to “Disabled.”
7. Click Apply to save your changes.



Note: If you are configuring the firewall from a wireless computer and you change the firewall’s SSID, channel, or security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the firewall’s new settings.

8. Configure and test your computers for wireless connectivity.

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

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

How to Restricting Wireless Access to Your Network

By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network. For increased security, the 54 Mbps Mobile Broadband Router MBR814 provides several ways to restrict wireless access to your network:

- Turn off wireless connectivity completely
- Restrict access based on the Wireless Network Name (SSID)
- Restrict access based on the Wireless Card Access List

These options are discussed below.

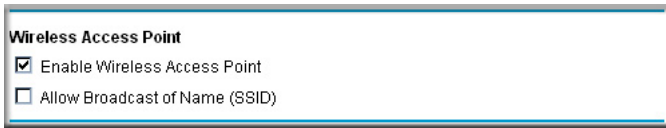


Figure 4-3: Wireless Access Point settings

Restricting Access to Your Network by Turning Off Wireless Connectivity

You can completely turn off the wireless portion of the MBR814. For example, if your notebook computer is used to wirelessly connect to your router and you take a business trip, you can turn off the wireless portion of the router while you are traveling. Other members of your household who use computers connected to the router via Ethernet cables will still be able to use the router.

Restricting Wireless Access Based on the Wireless Network Name (SSID)

The MBR814 can restrict wireless access to your network by not broadcasting the wireless network name (SSID). However, by default, this feature is turned off. If you turn this feature on, wireless devices will not ‘see’ your MBR814. You must configure your wireless devices to match the wireless network name (SSID) you configure in the MBR814 router.

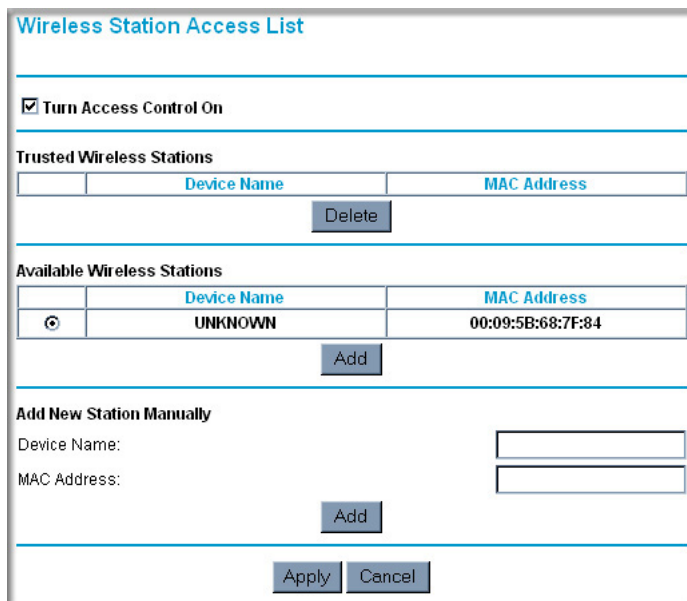
Note: The SSID of any wireless access adapters must match the SSID you configure in the 54 Mbps Mobile Broadband Router MBR814. If they do not match, you will not get a wireless connection to the MBR814.

Restricting Wireless Access Based on the Wireless Station Access List

This list determines which wireless hardware devices will be allowed to connect to the firewall.

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

1. Log in to the MBR814 firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. From the Wireless Settings menu, Wireless Station Access List section, click the Setup Access List button to display the list, shown below:



The screenshot shows the 'Wireless Station Access List' configuration page. At the top, there is a checkbox labeled 'Turn Access Control On' which is checked. Below this is a section titled 'Trusted Wireless Stations' containing an empty table with columns 'Device Name' and 'MAC Address', and a 'Delete' button. The next section is 'Available Wireless Stations', which contains a table with one entry: a radio button, 'UNKNOWN', and '00:09:5B:68:7F:84', with an 'Add' button below it. The final section is 'Add New Station Manually', featuring input fields for 'Device Name' and 'MAC Address', an 'Add' button, and 'Apply' and 'Cancel' buttons at the bottom.

Wireless Station Access List					
☒ Turn Access Control On					
Trusted Wireless Stations					
	<table border="1"><thead><tr><th>Device Name</th><th>MAC Address</th></tr></thead><tbody></tbody></table>	Device Name	MAC Address		
Device Name	MAC Address				
Delete					
Available Wireless Stations					
☒	<table border="1"><thead><tr><th>Device Name</th><th>MAC Address</th></tr></thead><tbody><tr><td>UNKNOWN</td><td>00:09:5B:68:7F:84</td></tr></tbody></table>	Device Name	MAC Address	UNKNOWN	00:09:5B:68:7F:84
Device Name	MAC Address				
UNKNOWN	00:09:5B:68:7F:84				
Add					
Add New Station Manually					
Device Name:					
MAC Address:					
Add					
Apply Cancel					

Figure 4-4: Wireless Access menu

3. Select the Turn Access Control On check box to enable restricting wireless computers by their MAC addresses.
4. If the wireless station is currently connected to the network, you can select it from the Available Wireless Stations list. Click Add to add the station to the Trusted Wireless Stations list.
5. If the wireless station is not currently connected, you can enter its address manually. Enter the MAC address of the authorized computer. The MAC address is usually printed on the wireless card, or it may appear in the router's DHCP table. The MAC address will be 12 hexadecimal digits.

Click Add to add your entry. You can add several stations to the list, but the entries will be discarded if you do not click Apply.

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



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

6. Make sure the Turn Access Control On check box is selected, then click Apply.

Now, only devices on this list will be allowed to wirelessly connect to the MBR814. This prevents unauthorized access to your network.

Choosing WEP Authentication and Security Encryption Methods

Figure 4-5. Security Encryption section

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

Authentication Type Selection

The MBR814 lets you select the following wireless authentication schemes.

- Automatic

- Open System
- Shared key



Note: The authentication scheme is separate from the data encryption. You can choose an authentication scheme which requires a shared key but still leave the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

Set your wireless adapter according to the authentication scheme you choose for the MBR814 router. Please refer to [“Authentication and WEP Data Encryption” on page D-2](#) for a full explanation of each of these options, as defined by the IEEE 802.11g wireless communication standard.

Encryption Choices

Please refer to [“Overview of WEP Parameters” on page D-5](#) for a full explanation of each of the following choices, as defined by the IEEE 802.11g wireless communication standard. Choose the encryption strength from the drop-down list:

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

64 or 128 bit WEP. When 64 Bit WEP or 128 Bit WEP is selected, WEP encryption will be applied.

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

There are two methods for creating WEP encryption keys:

- **Passphrase.** Enter a word or group of printable characters in the Passphrase box and click the Generate button.
- **Manual.** 64-bit WEP: Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F).
128-bit WEP: Enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

Select the radio button for the key you want to make active.

How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the MBR814 firewall at its default LAN address of <http://192.168.0.1> with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless Settings link in the main menu of the MBR814 router.
3. Go to the Security Encryption portion of the page:

Figure 4-6. Wireless WEP menu

4. Select the Authentication Type.
5. Select the Encryption setting.
6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network.
 - Automatic — enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
 - Manual — enter hexadecimal digits (any combination of 0-9, a-f, or A-F). Select which of the four keys will be active.
7. Select the radio button for the key you want to make active.

Be sure you clearly understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one included in Windows XP only allow entry of one key which must match the default key you set in the MBR814.

- Click Apply to save your settings.



Note: When configuring the router from a wireless computer, if you configure WEP settings, you will lose your wireless connection when you click Apply. You must then either configure your wireless adapter to match the router WEP settings or access the router from a wired computer to make any further changes.

How to Configure WPA-PSK

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK, follow these steps:

- Log in at the default LAN address of <http://192.168.0.1>, with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
- Click **Wireless Settings** in the Setup section of the main menu of the MBR814.
- Choose the **WPA-PSK** radio button. The WPA-PSK menu will open.
- Enter the pre-shared key in the Passphrase field.
- Click **Apply** to save your settings.

Chapter 5

Protecting Your Network

This chapter describes how to use the basic firewall features of the 54Mbps Mobile Broadband Router MBR814 to protect your network.

Protecting Access to Your 54Mbps Mobile Broadband Router MBR814

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

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

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

How to Change the Built-In Password

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



Figure 5-1: Log in to the router

2. From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in [Figure 5-2](#).

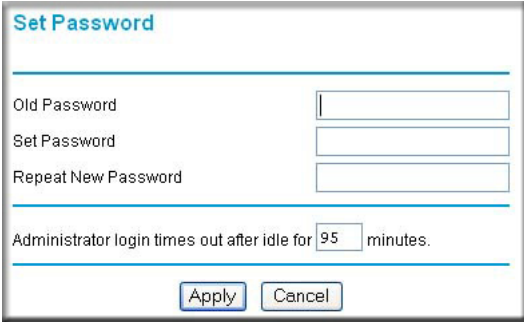
A screenshot of the 'Set Password' configuration window. The window has a title bar and a blue header with the text 'Set Password'. Below the header, there are three input fields: 'Old Password', 'Set Password', and 'Repeat New Password'. Below these fields is a line with the text 'Administrator login times out after idle for' followed by a text box containing the number '95' and the word 'minutes.'. At the bottom of the window are two buttons: 'Apply' and 'Cancel'.

Figure 5-2: Set Password menu

3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

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

Changing the Administrator Login Timeout

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

1. In the Set Password menu, type a number in 'Administrator login times out' field. The suggested default value is 5 minutes.
2. Click **Apply** to save your changes or click Cancel to keep the current period.

Configuring Basic Firewall Services

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

Blocking Keywords, Sites, and Services

The router provides a variety of options for blocking Internet based content and communications services. With its content filtering feature, the MBR814 router prevents objectionable content from reaching your PCs. The router allows you to control access to Internet content by screening for keywords within Web addresses. Key content filtering options include:

- Keyword blocking of HTTP traffic.
- Outbound Service Blocking limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of Service (DoS) protection. Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

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

How to Block Keywords and Sites

The MBR814 router allows you to restrict access to Internet content based on functions such as Web addresses and Web address keywords.

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. Select the Block Sites link of the Security menu.

The screenshot shows the 'Block Sites' configuration page. At the top, the title 'Block Sites' is in blue. Below it, the 'Keyword Blocking' section has three radio buttons: 'Never', 'Per Schedule', and 'Always', with 'Always' selected. A text input field labeled 'Type Keyword or Domain Name Here.' is followed by an 'Add Keyword' button. Below this is a list box titled 'Block Sites Containing these Keywords or Domain Names:' which is currently empty. At the bottom of the list box are 'Delete Keyword' and 'Clear List' buttons. Further down, there is a checkbox labeled 'Allow Trusted IP Address to Visit Blocked Sites' which is unchecked. Below the checkbox is a 'Trusted IP Address' field with four input boxes for IP octets. At the very bottom are 'Apply' and 'Cancel' buttons.

Figure 5-3: Block Sites menu

3. To enable keyword blocking, select one of the following:
 - Per Schedule—to turn on keyword blocking according to the settings on the Schedule page.
 - Always—to turn on keyword blocking all of the time, independent of the Schedule page.
4. Enter a keyword or domain in the Keyword box, click Add Keyword, then click Apply.

Some examples of Keyword application follow:

- If the keyword “XXX” is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the keyword “.com” is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
- Enter the keyword “.” to block all Internet browsing access.

Up to 32 entries are supported in the Keyword list.

5. To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.
6. To specify a trusted user, enter that computer’s IP address in the Trusted IP Address box and click **Apply**.

You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.

7. Click **Apply** to save your settings.

Firewall Rules

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

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the MBR814 are:

- Inbound: Block all access from outside except responses to requests from the LAN side.
- Outbound: Allow all access from the LAN side to the outside.

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

You can change the order of precedence of rules so that the rule that applies most often will take effect first. See [“Order of Precedence for Rules” on page 5-11](#) for more details.

To access the rules configuration of the MBR814, click the Firewall Rules link on the main menu, then click Add for either an Outbound or Inbound Service.

Firewall Rules

Outbound Services

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

Add Edit Move Delete

Inbound Services

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

Add Edit Move Delete

Apply Cancel

Figure 5-4: Rules menu

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

Inbound Rules (Port Forwarding)

Because the MBR814 uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.



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

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

Inbound Rule Example: A Local Public Web Server

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

The screenshot shows the 'Inbound Services' configuration window. It has a title bar 'Inbound Services' in blue. Below the title bar, there are several fields and dropdown menus. The 'Service' dropdown is set to 'HTTP (TCP:80)'. The 'Action' dropdown is set to 'ALLOW always'. The 'Send to LAN Server' field is set to '192.168.0.99'. The 'WAN Users' dropdown is set to 'Any'. Below 'WAN Users', there are 'start' and 'finish' time fields, both set to '0.0.0.0'. The 'Log' dropdown is set to 'Never'. At the bottom of the window, there are three buttons: 'Back', 'Apply', and 'Cancel'.

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

The parameters are:

- **Service**
From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services menu to add any additional services or applications that do not already appear.
- **Action**
Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **Send to LAN Server**
Enter the IP address of the computer or server on your LAN which will receive the inbound traffic covered by this rule.
- **WAN Users**
These settings determine which packets are covered by the rule, based on their source (WAN) IP address. Select the desired option:

- Any — all IP addresses are covered by this rule.
 - Address range — if this option is selected, you must enter the Start and Finish fields.
 - Single address — enter the required address in the Start field.
- Log

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

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

Inbound Rule Example: Allowing Videoconferencing

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in [Figure 5-6](#), CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.

The screenshot shows the 'Inbound Services' configuration window. The 'Service' dropdown is set to 'CU-SEEME(TCP/UDP:7648)'. The 'Action' dropdown is set to 'ALLOW always'. The 'Send to LAN Server' field contains the IP address '192.168.0.11'. The 'WAN Users' section has a dropdown set to 'Address Range'. Below this, the 'start' field is '134.177.88.1' and the 'finish' field is '134.177.88.254'. The 'Log' dropdown is set to 'Not Match'. At the bottom are 'Back', 'Apply', and 'Cancel' buttons.

Figure 5-6: Rule example: Videoconference from Restricted Addresses

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menu so that external users can always find your network.
- If the IP address of the local server computer is assigned by DHCP, it may change when the computer is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the computer's IP address constant.
- Local computers must access the local server using the computer's local LAN address (192.168.0.11 in the example in [Figure 5-6](#) above). Attempts by local computers to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The MBR814 allows you to block the use of certain Internet services by computers on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local computer based on:

- IP address of the local computer (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Following is an application example of outbound rules:

Outbound Rule Example: Blocking Instant Messenger

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

Outbound Services

Service: AIM(TCP:5190)

Action: BLOCK by schedule, otherwise allow

LAN users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

WAN Users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Match

Back Apply Cancel

Figure 5-7: Rule example: Blocking Instant Messenger

The parameters are:

- **Service**
From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Add Custom Service feature to add any additional services or applications that do not already appear.
- **Action**
Choose how you want this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **LAN Users**
These settings determine which packets are covered by the rule, based on their source LAN IP address. Select the desired option:
 - Any — all IP addresses are covered by this rule.
 - Address range — if this option is selected, you must enter the Start and Finish fields.
 - Single address — enter the required address in the Start field.

- **WAN Users**
These settings determine which packets are covered by the rule, based on their destination WAN IP address. Select the desired option:
 - Any — all IP addresses are covered by this rule.
 - Address range —if this option is selected, you must enter the Start and Finish fields.
 - Single address — enter the required address in the Start field.
- **Log**
You can select whether the traffic will be logged. The choices are:
 - Never — no log entries will be made for this service.
 - Always — any traffic for this service type will be logged.
 - Match — traffic of this type that matches the parameters and action will be logged.
 - Not match — traffic of this type that does not match the parameters and action will be logged.

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in [Figure 5-8](#):

Outbound Services							
	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
☐	1	☒	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never
Add Edit Move Delete							
Inbound Services							
	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
☒	1	☒	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
☐	2	☒	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match
Add Edit Move Delete							

Figure 5-8: Rules table with examples

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

Services

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

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the MBR814 already holds a list of many service port numbers, you are not limited to these choices. Use the procedure below to create your own service definitions.

How to Define Services

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. Select the Services link of the Security menu to display the Services menu shown in [Figure 5-9](#):

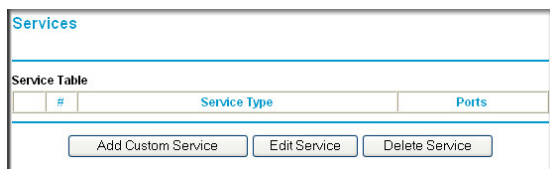


Figure 5-9: Services menu

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

- To edit an existing Service, select its button on the left side of the table and click Edit Service.
 - To delete an existing Service, select its button on the left side of the table and click Delete Service.
3. Use the page shown below to define or edit a service.

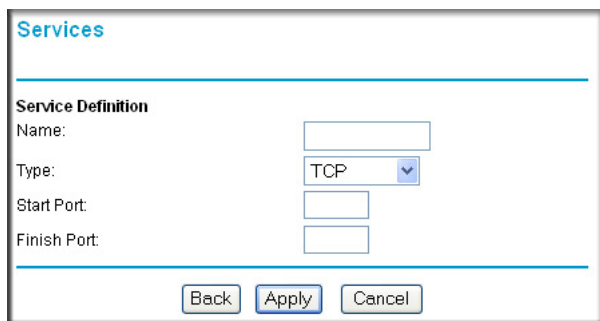


Figure 5-10: Add Services menu

4. Click Apply to save your changes.

Setting Times and Scheduling Firewall Services

The MBR814 router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet.

How to Set Your Time Zone

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

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. Select the Schedule link of the Security menu to display menu shown below.

The screenshot shows a web form titled "Schedule". It contains several sections: "Days:" with checkboxes for "Every Day", "Sunday", "Monday", "Tuesday", "Wednesday", "Thursday", "Friday", and "Saturday", all of which are checked. "Time of day: (use 24-hour clock)" with a checked "All Day" option and input fields for "Start Time" and "End Time", each with "Hour" and "Minute" sub-fields. "Time Zone" with a dropdown menu showing "(GMT) Greenwich Mean Time : Edinburgh, London" and two unchecked checkboxes for "Adjust for Daylight Savings Time" and "Use this NTP Server". Below these is a "Current Time:" label showing "2002-09-10 02:42:17". At the bottom are "Apply" and "Cancel" buttons.

Figure 5-11: Schedule Services menu

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

Select the Adjust for daylight savings time check box if your time zone is currently in daylight savings time.

4. The router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, enter its IP address under Use this NTP Server.
5. Click **Apply** to save your settings.

How to Schedule Firewall Services

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

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

2. Select the Schedule link of the Security menu to display menu shown above in the [Schedule Services](#) menu.
3. To block Internet services based on a schedule, select Every Day or select one or more days. If you want to limit access completely for the selected days, select All Day. Otherwise, to limit access during certain times for the selected days, enter Start Blocking and End Blocking times.

Note: Enter the values in 24-hour time format. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.

4. Click **Apply** to save your changes.

Chapter 6

Managing Your Network

This chapter describes how to perform network management tasks with your 54Mbps Mobile Broadband Router MBR814.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the MBR814 router are stored in a configuration file in the router. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.

How to Back Up the Configuration to a File

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Maintenance heading of the Main Menu, select the Backup Settings menu as seen in [Figure 6-1](#).

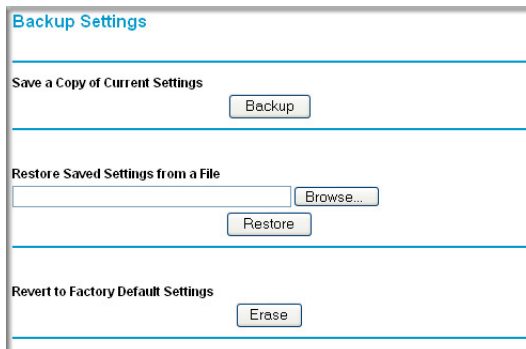


Figure 6-1: Backup Settings menu

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

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

How to Restore the Configuration from a File

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in [Figure 6-1](#).
3. Enter the full path to the file on your network or click the Browse button to locate the file.
4. When you have located the `.cfg` file, click the Restore button to upload the file to the router.
5. The router will then reboot automatically.

How to Erase the Configuration

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

1. To erase the configuration, from the Maintenance menu Settings Backup link, click the Erase button on the screen.
2. The router will then reboot automatically.

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.

Note: To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the router. See [“MBR814 Rear Panel” on page 2-6](#).

Upgrading the Router's Firmware

The software of the MBR814 router is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

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

How to Upgrade the Router Firmware

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

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

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

2. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
3. From the Main Menu of the browser interface, under the Maintenance heading, select the **Router Upgrade** heading to display the menu shown in [Figure 6-2](#).

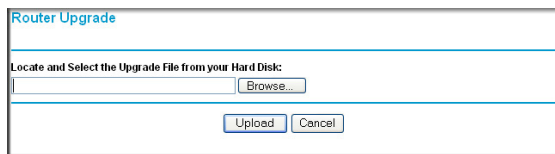


Figure 6-2: Router Upgrade menu

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



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

Network Management Information

The MBR814 provides a variety of status and usage information which is discussed below.

Viewing Router Status and Usage Statistics

From the Main Menu, under Maintenance, select Router Status to view the screen in [Figure 6-3](#).

Router Status	
Account Name	
Firmware Version	0.01.14
ADSL Port	
MAC Address	00:09:5b:70:46:26
IP Address	63.199.31.112
DHCP	PPPOE
IP Subnet Mask	255.255.255.255
Domain Name Server	206.13.31.12
LAN Port	
MAC Address	00:09:5b:70:46:26
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
Modem	
ADSL Firmware Version	1.00.05.00
Modem Status	Connected
DownStream Connection Speed	1536 kbps
UpStream Connection Speed	160 kbps
VPI	0
VCI	35
Show Statistics Connection Status	

Figure 6-3: Router Status screen

The Router Status menu provides status and usage information.

This screen shows the following parameters:

Table 6-1. Menu 3.2 - Router Status Fields

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

Click the Show Statistics button to display router usage statistics, as shown in [Figure 6-3](#) below:

The screenshot shows a web interface for router statistics. At the top, it says 'System Up Time 22:51:11'. Below this is a table with 8 columns: Port, Status, TxPkts, RxPkts, Collisions, Tx B/s, Rx B/s, and Up Time. There are two rows of data: WAN (ADSL) and LAN (10M/100M). Below the table, there is a 'Poll Interval' section with a text input set to '5', a '(secs)' label, a 'Set Interval' button, and a 'Stop' button.

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	ADSL	105159	179491	0	0	0	22:51:11
LAN	10M/100M	236651	249474	0	12	12	22:51:11

Poll Interval : (secs)

Figure 6-4: Router Statistics screen

This screen shows the following statistics:.

Table 6-1. Router Statistics Fields

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

Click the Connection Status button to display router connection status, as shown in [Figure 6-5](#) and [Figure 6-6](#).

Connection Status

IP Address	192.168.2.54
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DHCP Server	192.168.2.54
DNS Server	66.125.125.214
Lease Obtained	2003-08-27 08:09:58
Lease Expires	2003-08-26 23:37:32

Release Renew

Close Window

Figure 6-5: Connection Status screen for Dynamic IP

Clicking the Renew button updates the status information.

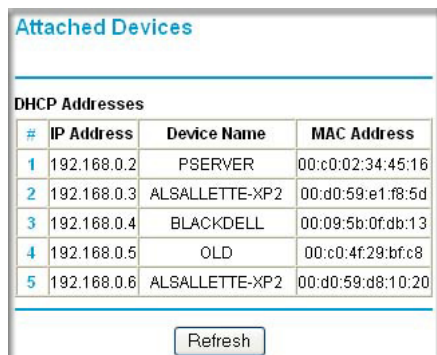
This screen shows the following statistics:

Table 6-1. Connection Status Fields for Dynamic IP

Field	Description
IP Address	The IP Address assigned to the WAN port by the ADSL Internet Service Provider.
Subnet Mask	The Network Mask assigned to the WAN port by the ADSL Internet Service Provider.
Default Gateway	The default gateway router assigned to the WAN port by the ADSL Internet Service Provider.
DHCP Server	The DHCP server's IP address.
DNS Server	The DNS server's IP address.
Lease Obtained	Date and time the lease was obtained.
Lease Expires	Date and time the lease expires.

Viewing Attached Devices

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



DHCP Addresses			
#	IP Address	Device Name	MAC Address
1	192.168.0.2	PSEVER	00:c0:02:34:45:16
2	192.168.0.3	ALSALLETTE-XP2	00:d0:59:e1:f8:5d
3	192.168.0.4	BLACKDELL	00:09:5b:0f:db:13
4	192.168.0.5	OLD	00:c0:4f:29:bf:c8
5	192.168.0.6	ALSALLETTE-XP2	00:d0:59:d8:10:20

Refresh

Figure 6-6: Attached Devices menu

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

Viewing, Selecting, and Saving Logged Information

The router will log security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites menu, the Logs page can show you when someone on your network tries to access a blocked site. If you enabled e-mail notification, you will receive these logs in an e-mail message. If you do not have e-mail notification enabled, you can view the logs here.

An example of the logs file is shown below.

Logs

Current time: 2003-08-26 07:42:13

Tue, 2003-08-26 06:04:14	- Send out NTP request
Tue, 2003-08-26 06:04:14	- Receive NTP Reply
Tue, 2003-08-26 07:17:17	- Administrator login
Tue, 2003-08-26 07:26:19	- Administrator login
Tue, 2003-08-26 07:26:32	- Administrator login
Tue, 2003-08-26 07:29:48	- Administrator login
Tue, 2003-08-26 07:38:12	- TCP Packet - Source
Tue, 2003-08-26 07:38:39	- ICMP Packet - Source
Tue, 2003-08-26 07:38:42	- TCP Packet - Source
Tue, 2003-08-26 07:39:43	- TCP Packet - Source
Tue, 2003-08-26 07:39:49	- ICMP Packet - Source
Tue, 2003-08-26 07:39:49	- TCP Packet - Source
Tue, 2003-08-26 07:41:29	- TCP Packet - Source

Refresh Clear Log Send Log

Include in Log

- ☒ Attempted access to blocked sites
- ☒ Connections to the Web-based interface of this Router
- ☒ Router operation (start up, get time etc)
- ☒ Known DoS attacks and Port Scans

Syslog

☒ Disable

☐ Broadcast on LAN

☐ Send to this Syslog server IP address . . .

Apply Cancel

Figure 6-7: Security Logs menu

Log entries are described in [Table 6-1](#) below:

Table 6-1. Security Log entry descriptions

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

Log action buttons are described in [Table 6-2](#) below:

Table 6-2. Security Log action buttons

Field	Description
Refresh	Refresh the log screen.
Clear Log	Clear the log entries.
Send Log	Email the log immediately.
Apply	Apply the current settings.
Cancel	Clear the current settings.

Selecting What Information to Log

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

- Attempted access to blocked site
- Connections to the Web-based interface of the router
- Router operation (start up, get time, etc.)
- Known DoS attacks and Port Scans

Saving Log Files on a Server

You can choose to write the logs to a computer running a syslog program. To activate this feature, select to Broadcast on Lan or enter the IP address of the server where the Syslog file will be written.

Examples of Log Messages

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

Activation and Administration

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

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

Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2

Thu, 2002-05-21 18:56:58 - Administrator logout - IP:192.168.0.2

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

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

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

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

[This entry shows when the log was emailed.]

Dropped Packets

Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN - Destination:134.177.0.11,21,LAN - [Inbound Default rule match]

Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN - Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]

Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN - Destination:134.177.0.11,0,LAN - [Inbound Default rule match]

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

Enabling Security Event E-mail Notification

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

The screenshot shows a web-based configuration interface for an E-mail subheading. It includes a checkbox for 'Turn E-mail Notification On'. Below this, there are two text input fields for 'Outgoing Mail Server' and 'Send To This E-mail Address'. A section titled 'Send E-Mail alerts immediately' contains three checked checkboxes for 'If a DoS attack is detected.', 'If a Port Scan is detected.', and 'If someone attempts to access a blocked site.'. Another section titled 'Send Logs According to this Schedule' has a dropdown menu set to 'Hourly', a 'Day' dropdown, and a 'Time' dropdown with radio buttons for 'a.m.' and 'p.m.'. At the bottom are 'Apply' and 'Cancel' buttons.

Figure 6-8: E-mail menu

- **Turn e-mail notification on.** Select this check box if you want to receive e-mail logs and alerts from the router.
- **Send alerts and logs via email.** Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.
- **Send alert immediately.** Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule.** Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
 - Day for sending log
Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.
 - Time for sending log
Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

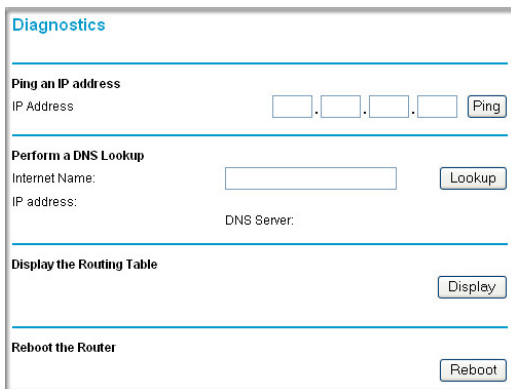
If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In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

Running Diagnostic Utilities and Rebooting the Router

The MBR814 router has a diagnostics feature. You can use the diagnostics menu to perform the following functions from the router:

- Ping an IP Address to test connectivity to see if you can reach a remote host.
- Perform a DNS Lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing Table to identify what other routers the router is communicating with.
- Reboot the router to enable new network configurations to take effect or to clear problems with the router's network connection.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Diagnostics heading to display the menu shown in [Figure 6-9](#).



The screenshot shows a web browser interface for the router's diagnostics menu. It has a title bar 'Diagnostics' in blue. Below it are four sections separated by horizontal lines. The first section is 'Ping an IP address' with a label 'IP Address' and a form with four input boxes for IP digits and a 'Ping' button. The second section is 'Perform a DNS Lookup' with labels 'Internet Name:' and 'IP address:' next to a single input box, and a 'DNS Server:' label with no input. There is a 'Lookup' button. The third section is 'Display the Routing Table' with a 'Display' button. The fourth section is 'Reboot the Router' with a 'Reboot' button.

Figure 6-9: Diagnostics menu

Enabling Remote Management

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your 54Mbps Mobile Broadband Router MBR814.



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

Configuring Remote Management

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Advanced section of the main menu, select the Remote Management link.
3. Select the Turn Remote Management On check box.
4. Specify what external addresses will be allowed to access the router's remote management. For security, restrict access to as few external IP addresses as practical:
 - To allow access from any IP address on the Internet, select Everyone.
 - To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.
 - To allow access from a single IP address on the Internet, select Only this Computer. Enter the IP address that will be allowed access.
5. Specify the Port Number that will be used for accessing the management interface.

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

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

`http://134.177.0.123:8080`

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

Chapter 7

Advanced Configuration

This chapter describes how to configure the advanced features of your 54Mbps Mobile Broadband Router MBR814.

Configuring Advanced Security

The 54Mbps Mobile Broadband Router MBR814 provides a variety of advanced features, such as:

- Setting up a Demilitarized Zone (DMZ) Server
- Connecting Automatically, as Required
- Disabling Port Scan and DOS Protection
- Responding to a Ping on the Internet WAN Port
- MTU Size
- Flexibility on configuring your LAN TCP/IP settings
- Using the Router as a DHCP Server
- Configuring Dynamic DNS
- Configuring Static Routes

These features are discussed below.

Setting Up A Default DMZ Server

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



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

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

How to Configure a Default DMZ Server

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

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. From the Main Menu, under Advanced, click the WAN Setup link to view the page shown in [Figure 7-1](#):

WAN Setup

☒ Connect Automatically, as Required

☐ Disable Port Scan and DOS Protection

☐ Default DMZ Server 192 . 168 . 0 .

☐ Respond to Ping on Internet WAN Port

MTU Size (in bytes) 1492

Apply Cancel

Figure 7-1: WAN Setup Page

3. Select the Default DMZ Server check box.
4. Type the IP address for that server.
5. Click **Apply** to save your changes.

Connect Automatically, as Required

Normally, this option should be enabled, so that an Internet connection will be made automatically, whenever Internet-bound traffic is detected. If this causes high connection costs, you can disable this setting.

If disabled, you must connect manually, using the sub-screen accessed from the "Connection Status" button on the Status screen.

If you have an "Always on" connection, this setting has no effect.

Disable Port Scan and DOS Protection

The Firewall protects your LAN against Port Scans and Denial of Service (DOS) attacks. This should be disabled only in special circumstances.

Respond to Ping on Internet WAN Port

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

MTU Size

The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes, or 1492 Bytes for PPPoE connections. For some ISPs you may need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Configuring LAN IP Settings

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

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

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

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

LAN IP Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: Disable

☒ Use Router as DHCP Server

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	MAC Address
---	------------	-------------	-------------

Add Edit Delete

Apply Cancel

Figure 7-2: LAN IP Setup Menu

The LAN TCP/IP Setup parameters are:

- **IP Address**
This is the LAN IP address of the router.
- **IP Subnet Mask**
This is the LAN Subnet Mask of the router. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
- **RIP Direction**
RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the Router sends and receives RIP packets. Both is the default.
 - When set to Both or Out Only, the router will broadcast its routing table periodically.
 - When set to Both or In Only, it will incorporate the RIP information that it receives.
 - When set to None, it will not send any RIP packets and will ignore any RIP packets received.
- **RIP Version**
This controls the format and the broadcasting method of the RIP packets that the router sends. It recognizes both formats when receiving. By default, this is set for RIP-1.

- RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
- RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
 - RIP-2B uses subnet broadcasting.
 - RIP-2M uses multicasting.



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.

DHCP

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

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. See [“IP Configuration by DHCP” on page B-9](#) for an explanation of DHCP and information about how to assign IP addresses for your network.

Use Router as DHCP server

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

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the router’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you may want to save part of the range for devices with fixed addresses.

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

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address is the router’s LAN IP address

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

Reserved IP addresses

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

To reserve an IP address:

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

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

To edit or delete a reserved address entry:

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

How to Configure LAN TCP/IP Settings

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

- From the Main Menu, under Advanced, click the LAN IP Setup link to view the menu, shown in [Figure 7-3](#):

LAN IP Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: None

RIP Version: Disable

☒ **Use Router as DHCP Server**

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 254

Address Reservation

#	IP Address	Device Name	MAC Address

Add Edit Delete

Apply Cancel

Figure 7-3: LAN IP Setup Menu

- Enter the TCP/IP, DHCP, or Reserved IP parameters.
- Click **Apply** to save your changes.

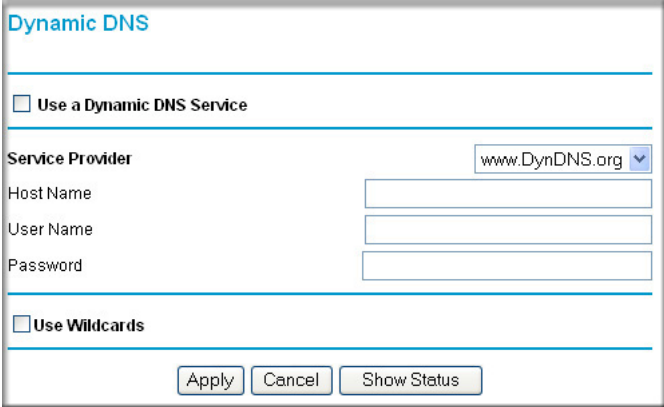
Configuring Dynamic DNS

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

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

How to Configure Dynamic DNS

1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, select Dynamic DNS to display the page below.



The screenshot shows a web form titled "Dynamic DNS". At the top, there is a checkbox labeled "Use a Dynamic DNS Service". Below this, there is a section for "Service Provider" with a dropdown menu currently showing "www.DynDNS.org". Underneath the dropdown are three text input fields labeled "Host Name", "User Name", and "Password". At the bottom of the form, there is another checkbox labeled "Use Wildcards". Below the checkboxes are three buttons: "Apply", "Cancel", and "Show Status".

Figure 7-4: Dynamic DNS menu

3. Access the Web site of one of the dynamic DNS service providers whose names appear in the 'Service Provider' box, and register for an account.
For example, for dyndns.org, go to www.dyndns.org.
4. Select the "Use a dynamic DNS service" check box.
5. Select the name of your dynamic DNS Service Provider.
6. Type the Host Name that your dynamic DNS service provider gave you.
The dynamic DNS service provider may call this the domain name. If your URL is myName.dyndns.org, then your Host Name is "myName."
7. Type the User Name for your dynamic DNS account.
8. Type the Password (or key) for your dynamic DNS account.
9. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the Use wildcards check box to activate this feature.
For example, the wildcard feature will cause [*.yourhost.dyndns.org](http) to be aliased to the same IP address as [yourhost.dyndns.org](http)

10. Click **Apply** to save your configuration.



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

Using Static Routes

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

Static Route Example

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

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's 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 192.168.0.100. The static route would look like [Figure 7-6](#).

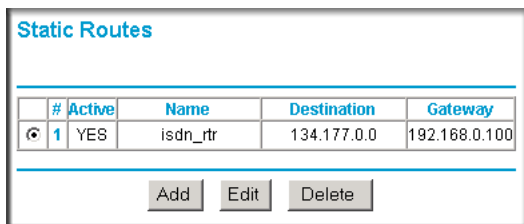
In this example:

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

- A Metric value of 1 will work since the ISDN router is on the LAN.
This represents the number of routers between your network and the destination. This is a direct connection so it is set to 1.
- Private is selected only as a precautionary security measure in case RIP is activated.

How to Configure Static Routes

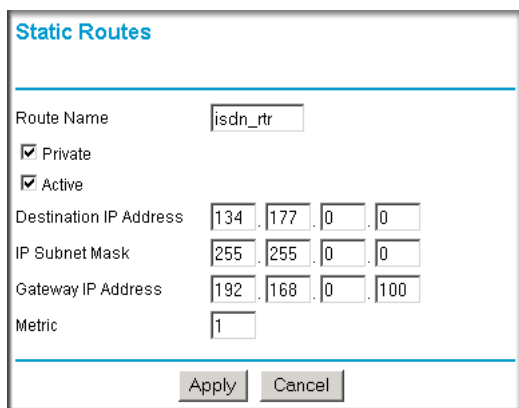
1. Log in to the router at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the router.
2. From the Main Menu of the browser interface, under Advanced, click Static Routes to view the Static Routes menu, shown in [Figure 7-5](#).



#	Active	Name	Destination	Gateway
1	YES	isdn_rtr	134.177.0.0	192.168.0.100

Figure 7-5: Static Routes Table

3. To add or edit a Static Route:
 - a. Click the **Edit** button to open the Edit Menu, shown in [Figure 7-6](#).



Static Routes

Route Name:

☒ Private

☒ Active

Destination IP Address: . . .

IP Subnet Mask: . . .

Gateway IP Address: . . .

Metric:

Figure 7-6: Static Route Entry and Edit Menu

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

Universal Plug and Play (UPnP)

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

1. Click UPnP on the main menu to invoke the UPnP menu:

UPnP

☒ Turn UPnP On

Advertisement Period (in minutes)

Advertisement Time To Live (in hops)

UPnP Portmap Table

Active	Protocol	Int. Port	Ext. Port	IP Address
--------	----------	-----------	-----------	------------

Apply Cancel Refresh

Figure 7-7: Universal Plug and Play menu

2. Fill out the UPnP screen:

- **Turn UPnP On:** UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If disabled, the Router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the Router.
- **Advertisement Period:** The Advertisement Period is how often the Router will advertise (broadcast) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations will ensure that control points have current device status at the expense of additional network traffic. Longer durations may compromise the freshness of the device status but can significantly reduce network traffic.
- **Advertisement Time To Live:** The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it may be necessary to increase this value a little.
- **UPnP Portmap Table:** The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the Router and which ports (Internal and External) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

3. To save, cancel or refresh the table:

- a. Click **Apply** to save the new settings to the Router.
- b. Click **Cancel** to disregard any unsaved changes.
- c. Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Chapter 8

Troubleshooting

This chapter gives information about troubleshooting your 54Mbps Mobile Broadband Router MBR814. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?
- Have I connected the router correctly?
Go to [“Basic Functioning” on page 8-1.](#)
- I can’t access the router’s configuration with my browser.
Go to [“Troubleshooting the Web Configuration Interface” on page 8-3.](#)
- I’ve configured the router but I can’t access the Internet.
Go to [“Troubleshooting the ISP Connection” on page 8-4.](#)
- I can’t remember the router’s configuration password.
- I want to clear the configuration and start over again.
Go to [“Restoring the Default Configuration and Password” on page 8-7.](#)

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 (see [“The Router’s Front Panel” on page 2-5](#) for an illustration and explanation of the LEDs).
2. Verify that the Test LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 10 seconds, verify that:
 - a. The Test LED is not lit.
 - b. The LAN port LEDs are lit for any local ports that are connected.
 - c. The WAN port LED is lit.

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

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

Power LED Not On

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

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

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

Test LED Never Turns On or Test LED Stays On

When the 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 Reset button” on page 8-7](#).

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

LAN or WAN Port LEDs Not On

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

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure the wireless broadband PC card is inserted properly.

Troubleshooting the Web Configuration Interface

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

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to [“Verifying TCP/IP Properties” on page C-6](#) or [“Verifying TCP/IP Properties for Macintosh Computers” on page C-17](#) to find your computer's IP address. Follow the instructions in [Appendix C](#) to configure your computer.

Note: If your computer's IP address is shown as 169.254.x.x:

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 computer to the router and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in [“Using the Reset button” on page 8-7](#).
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

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

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

Troubleshooting the ISP Connection

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

Internet LED Green or Blinking Green

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

Internet LED Off

If the Internet LED is off, disconnect the power to the router. Ensure the wireless broadband PC card is inserted properly and re-connect the power to the router.

If the problem persists, the wireless coverage in your area may be poor or the PC card may be defective.

Obtaining an Internet IP Address

If your router is unable to access the internet, and your Internet LED is green or blinking green, you should determine whether the router is able to obtain a Internet 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 check for your computer's host name.
Assign the computer Host Name of your ISP account to the router in the browser-based Setup Wizard.
- You have poor wireless coverage.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your computer's MAC address. In this case:
Inform your ISP that you have bought a new network device, and ask them to use the router's MAC address.

OR

Configure your router to spoof your computer's MAC address. This can be done in the Basic Settings menu. Refer to [“Manually Configuring Your Internet Connection” on page 3-7](#).

Troubleshooting Internet Browsing

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

- Your computer may not recognize any DNS server addresses.
A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the router's configuration, reboot your computer and verify the DNS address as described in [“Verifying TCP/IP Properties” on page C-6](#). Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.
- Your computer may not have the router configured as its TCP/IP router.
If your computer obtains its information from the router by DHCP, reboot the computer and verify the router address as described in [“Verifying TCP/IP Properties” on page C-6](#).

Troubleshooting a TCP/IP Network Using the Ping Utility

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

Testing the LAN Path to Your Router

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

To ping the router from a 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 port LED is on. If the LED is off, follow the instructions in [“LAN or WAN Port LEDs Not On”](#) on [page 8-2](#).
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
 - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer 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 router. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default router as described in [“Verifying TCP/IP Properties” on page C-6](#).
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your wireless broadband PC card is installed properly.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to “clone” or “spoof” the MAC address from the authorized PC. Refer to [“Manually Configuring Your Internet Connection” on page 3-7](#).

Restoring the Default Configuration and Password

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

- Use the Erase function of the Web Configuration Manager (see [“Backing Up, Restoring, or Erasing Your Settings” on page 6-1](#)).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

Using the Reset button

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

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).
2. Release the Default Reset button and wait for the router to reboot.

Problems with Date and Time

The E-mail menu in the Content Filtering section displays the current date and time of day. The MBR814 router uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000
Cause: The router has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least five minutes and check the date and time again.
- Time is off by one hour
Cause: The router does not automatically sense Daylight Savings Time. In the E-mail menu, check or uncheck the box marked “Adjust for Daylight Savings Time”.

Appendix A

Technical Specifications

This appendix provides technical specifications for the 54Mbps Mobile Broadband Router MBR814.

Network Protocol and Standards Compatibility

Data and Routing Protocols: TCP/IP, RIP-1, RIP-2, DHCP, RFC 1483 Bridged or Routed Ethernet

Power Adapter

North America: 120V, 60 Hz, input

United Kingdom, Australia: 240V, 50 Hz, input

Europe: 230V, 50 Hz, input

Japan: 100V, 50/60 Hz, input

All regions (output): 15 V AC @ 1.0A output, 24W maximum 12V DC @ 1.2A

Physical Specifications

Dimensions: 10" x 6.7" x 1.3"
255 mm x 169 mm x 34 mm

Weight: 1.4 lbs.
0.62 kg

Environmental Specifications

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

Operating humidity: 90% maximum relative humidity, noncondensing

Electromagnetic Emissions

Meets requirements of: FCC Part 15 Class B

Interface Specifications

LAN: 10BASE-T or 100BASE-Tx, RJ-45

WAN: PC Card Bus

Appendix B

Network and Routing Basics

This chapter provides an overview of IP networks and routing.

Related Publications

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

Basic Router Concepts

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

What is a Router?

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

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The 54Mbps Mobile Broadband Router MBR814 is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

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

The MBR814 router supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

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

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

For example, the following binary address:

```
11000011 00100010 00001100 00000111
```

is normally written as:

```
195.34.12.7
```

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

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

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

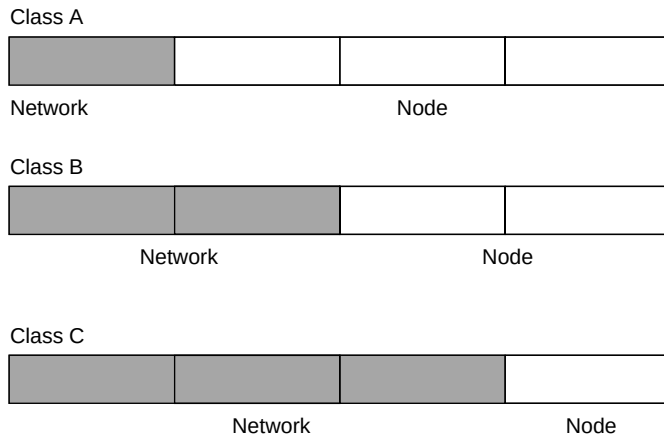


Figure B-1: Three Main Address Classes

The five address classes are:

- **Class A**
Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:
1.x.x.x to 126.x.x.x.
- **Class B**
Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:
128.1.x.x to 191.254.x.x.
- **Class C**
Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:
192.0.1.x to 223.255.254.x.
- **Class D**
Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:
224.0.0.0 to 239.255.255.255.
- **Class E**
Class E addresses are for experimental use.

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

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

Netmask

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

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

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

combined with:

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

Equals:

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

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

Subnet Addressing

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

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



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

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

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 192.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.



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

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

Table 8-1. Netmask Notation Translation Table for One Octet

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

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

Table 8-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

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 MBR814 router is preconfigured to automatically assign private addresses.

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

Single IP Address Operation Using NAT

In the past, if multiple 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 MBR814 router employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

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

The following figure illustrates a single IP address operation.

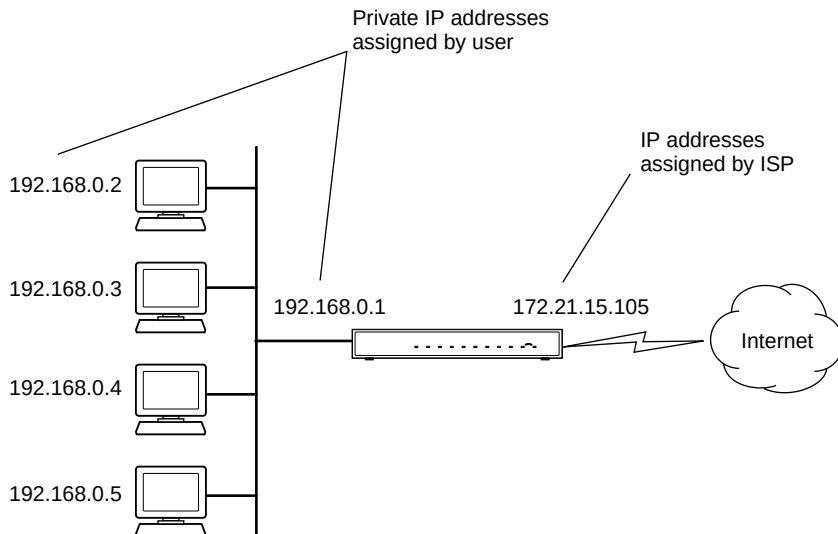


Figure B-3: Single IP Address Operation Using NAT

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

MAC Addresses and Address Resolution Protocol

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

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

Related Documents

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

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

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

Domain Name Server

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

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

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The MBR814 router has the capacity to act as a DHCP server.

The MBR814 router 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.

Internet Security and Firewalls

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

What is a Firewall?

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

Stateful Packet Inspection

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

Denial of Service Attack

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

Ethernet Cabling

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

Table B-1. UTP Ethernet cable wiring, straight-through

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

Category 5 Cable Quality

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

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

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

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

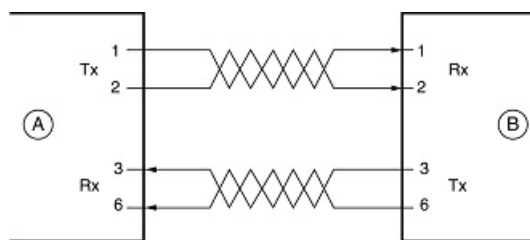
The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

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

Inside Twisted Pair Cables

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

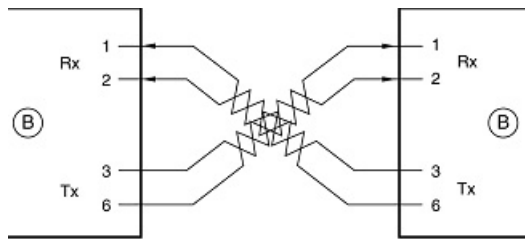
Figure B-4 illustrates straight-through twisted pair cable.



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

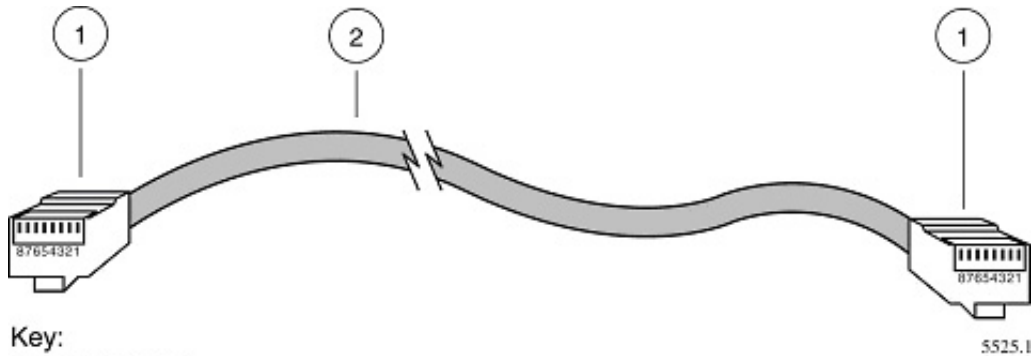
Figure B-4: Straight-Through Twisted-Pair Cable

Figure B-5 illustrates crossover twisted pair cable.



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

Figure B-5: Crossover Twisted-Pair Cable



Key:
 1 = RJ-45 plug
 2 = Category 5 UTP patch cable

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

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

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

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

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

The MBR814 router incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

Appendix C

Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the 54Mbps Mobile Broadband Router MBR814 and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).



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

Preparing Your Computers for TCP/IP Networking

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

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

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

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

The MBR814 router is shipped preconfigured as a DHCP server. The router 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 router)—192.168.0.1

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

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

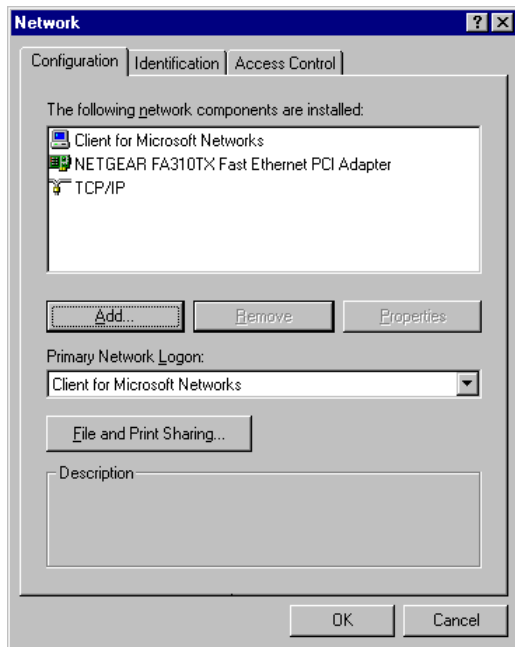
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Installing or Verifying Windows Networking Components

To install or verify the necessary components for IP networking:

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

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



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



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

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

- a. Click the Add button.
- b. Select Adapter, and then click Add.
- c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

- a. Click the Add button.
- b. Select Protocol, and then click Add.
- c. Select Microsoft.
- d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

- a. Click the Add button.
 - b. Select Client, and then click Add.
 - c. Select Microsoft.
 - d. Select Client for Microsoft Networks, and then click OK.
3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings in Windows 95B, 98, and Me

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

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

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

1

Locate your **Network Neighborhood** icon.

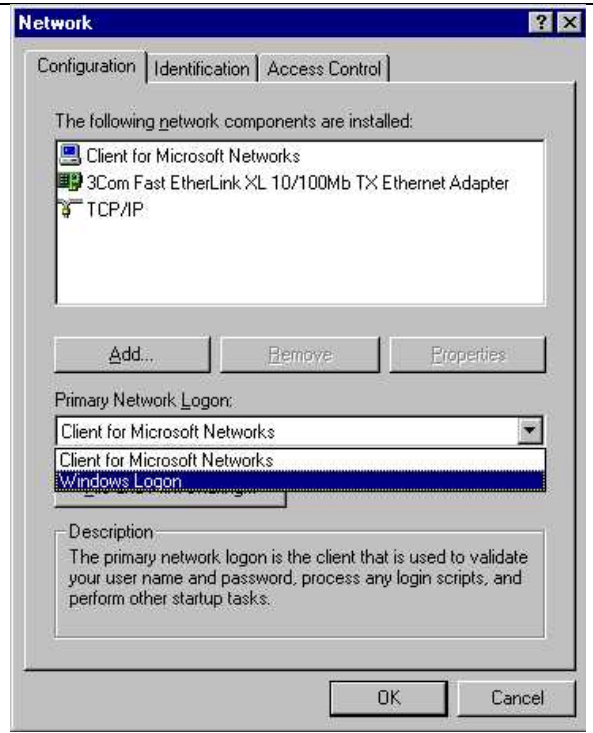
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
 - Click **Start** on the task bar located at the bottom left of the window.
 - Choose **Settings**, and then **Control Panel**.
 -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

2

Verify the following settings as shown:

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

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

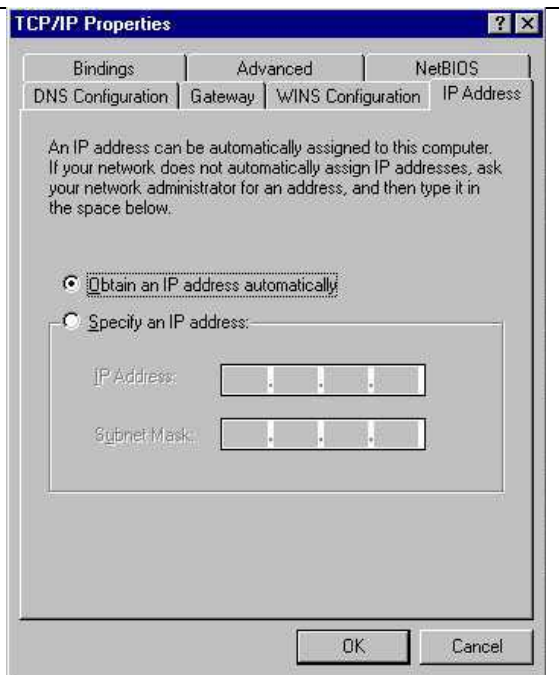


3

- By default, the **IP Address** tab is open on this window.
- Verify the following:
 - Obtain an IP address automatically** is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.
 - Click **OK** to continue.

Restart the PC.

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



Selecting the Windows' Internet Access Method

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

Verifying TCP/IP Properties

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

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

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

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

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

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

- The IP address is between 192.168.0.2 and 192.168.0.254
- The subnet mask is 255.255.255.0
- The default gateway is 192.168.0.1

Configuring Windows NT4, 2000 or XP for IP Networking

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

Installing or Verifying Windows Networking Components

To install or verify the necessary components for IP networking:

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

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

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

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

DHCP Configuration of TCP/IP in Windows XP

1

Locate your **Network Neighborhood** icon.

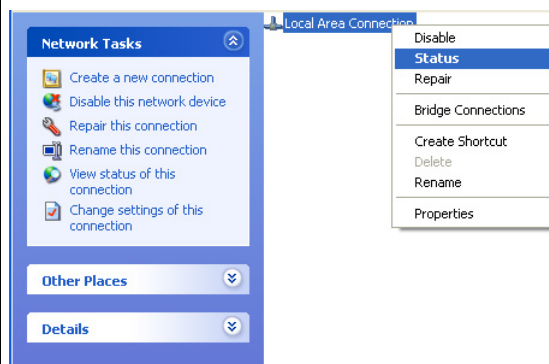
- Select **Control Panel** from the Windows XP new Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

2

- Now the Network Connection window displays.

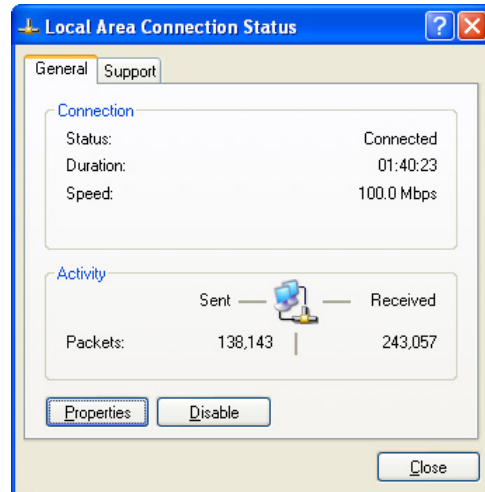
The Connections List that shows all the network connections set up on the PC, located to the right of the window.

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



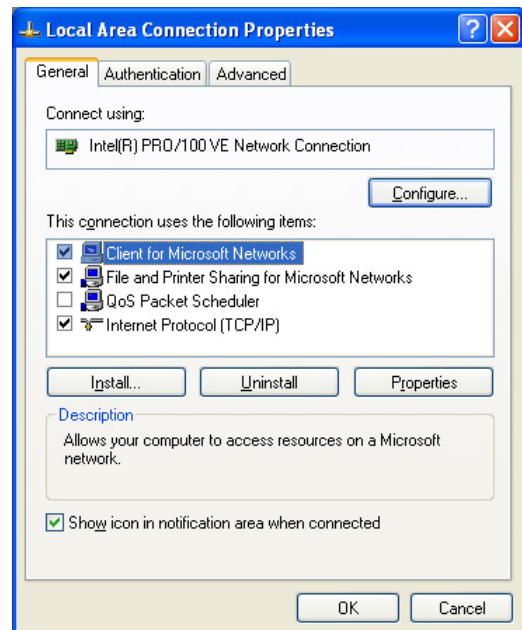
3

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



4

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

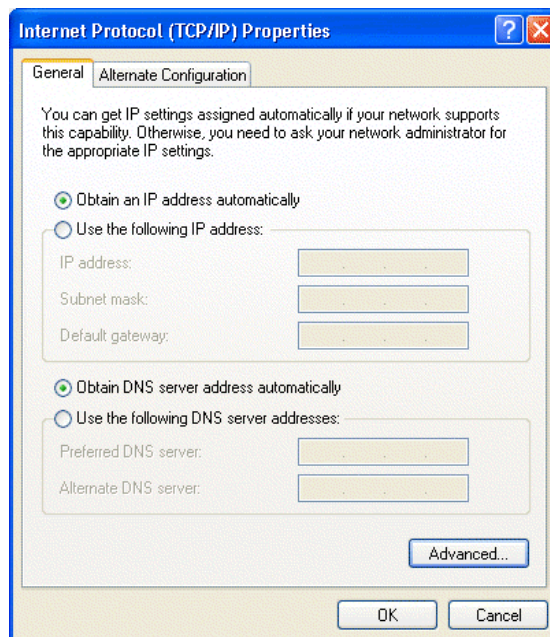


5

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

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

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



DHCP Configuration of TCP/IP in Windows 2000

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