

Reference Manual for the Mobile Broadband Router MBR814X



NETGEAR

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

202-10141-01
January 2006

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.

Operation is subject to the following two conditions:

- 1) this device may not cause interference and
- 2) this device must accept any interference, including interference that may cause undesired operation of the device

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.

Customer Support

Refer to the Support Information Card that shipped with your Mobile Broadband Router MBR814X.

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 is required.

Product and Publication Details

Model Number:	MBR814X
Publication Date:	January 2006
Product Family:	Product Family
Product Name:	Mobile Broadband Router MBR814X
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10141-01

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 collocated 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	2-2
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?	2-4
The Router's Front Panel	2-5
The Router's Rear Panel	2-6

Chapter 3

Connecting the Router to the Internet

Minimum Requirements	3-1
Ethernet Cabling Requirements	3-1
Computer Hardware Requirements	3-1
LAN Configuration Requirements	3-2
Internet Configuration Requirements	3-2
Where Do I Get the Internet Configuration Parameters?	3-2
Record Your Internet Connection Information	3-3
Connecting the MBR814X 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	3-8
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	4-6
How to Restricting Wireless Access to Your Network	4-7
Choosing WEP Authentication and Security Encryption Methods	4-9
How to Configure WEP	4-11
How to Configure WPA-PSK	4-12
Chapter 5	
Protecting Your Network	
Protecting Access to Your Mobile Broadband Router MBR814X.....	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
Outbound Rules (Service Blocking)	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	6-4
Viewing Router Status and Usage Statistics	6-4
Viewing Attached Devices	6-9
Viewing, Selecting, and Saving Logged Information	6-9
Examples of Log Messages	6-12
Enabling Security Event E-mail Notification	6-13
Running Diagnostic Utilities and Rebooting the Router	6-14
Enabling Remote Management	6-15
Configuring Remote Management	6-15

Chapter 7

Advanced Configuration

Configuring Advanced Security	7-1
Setting Up A Default DMZ Server	7-1
Connect Automatically, as Required	7-2
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
How to Configure LAN TCP/IP Settings	7-6
Using Static Routes	7-7
Static Route Example	7-7
How to Configure Static Routes	7-8
Universal Plug and Play (UPnP)	7-10

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
Wireless Broadband Link	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	
Related Documents	B1

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.
---	--

	Tip: This format is used to highlight a procedure that will save time or resources.
---	--

	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.
---	--



Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

This manual is written for the MBR814X router according to these specifications:

Table 1-2. Manual Scope






Product Version	Mobile Broadband Router MBR814X
Manual Publication Date	January 2006



Note: Product updates are available on the NETGEAR, Inc. Web site at <http://kbserver.netgear.com/products/MBR814X.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.
- 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 Mobile Broadband Router MBR814X. The MBR814X 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 the link to the document [“Internet Networking and TCP/IP Addressing”](#) in Appendix B to become more familiar with the terms and procedures used in this manual.

About the Router

The Mobile Broadband Router MBR814X provides continuous, high-speed 10/100 Ethernet access between your Ethernet devices. The MBR814X 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 MBR814X 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 MBR814X 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 MBR814X 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.
- Wireless access can be restricted by MAC address.

A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the MBR814X 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 MBR814X 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 MBR814X 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 MBR814X 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 MBR814X supports Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). See the link to [“Internet Networking and TCP/IP Addressing: in Appendix B](#) for further information on TCP/IP.

- **The Ability to Enable or Disable IP Address Sharing by NAT**
The MBR814X 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 MBR814X if you want to manage the IP address scheme yourself.
- **Automatic Configuration of Attached PCs by DHCP**
The MBR814X 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.
- **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 MBR814X 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:

- Mobile Broadband Router MBR814X
- 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 Mobile Broadband Router MBR814X front panel shown below contains status LEDs.

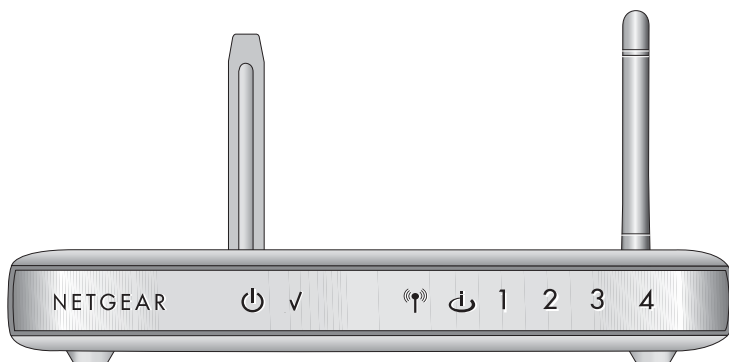







Figure 2-1

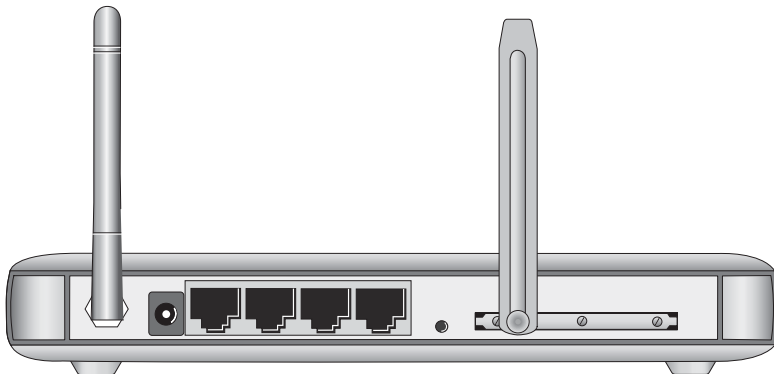
You can use the LEDs to verify various conditions. [Table 2-1](#) lists and describes each LED on the front panel of the router. These LEDs are green when lit.

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 Mobile Broadband Router MBR814 contains port connections.

**Figure 2-2**

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 MBR814X for Internet access.

Minimum Requirements

The MBR814X 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 [“Observe Performance, Placement, and Range Guidelines”](#) in Chapter 4.
- If connecting your computer to the router wirelessly, 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 MBR814X 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 MBR814X 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 see the link to [“Preparing a Computer for Network Access:”](#) in Appendix B 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 *MBR814X 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 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 MBR814X to Your LAN

This section provides instructions for connecting the MBR814X router.

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.

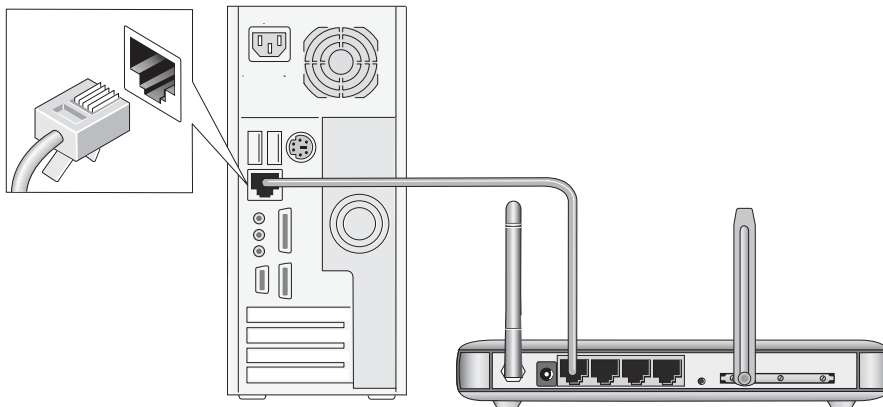




Figure 3-1

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 the link to [“Preparing a Computer for Network Access:”](#) in [Appendix B](#).

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.



Figure 3-2

A login window opens as shown below:

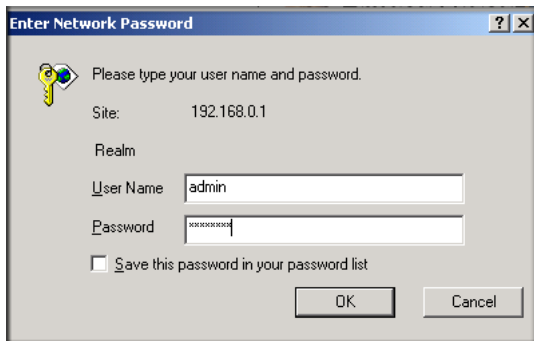


Figure 3-3

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.

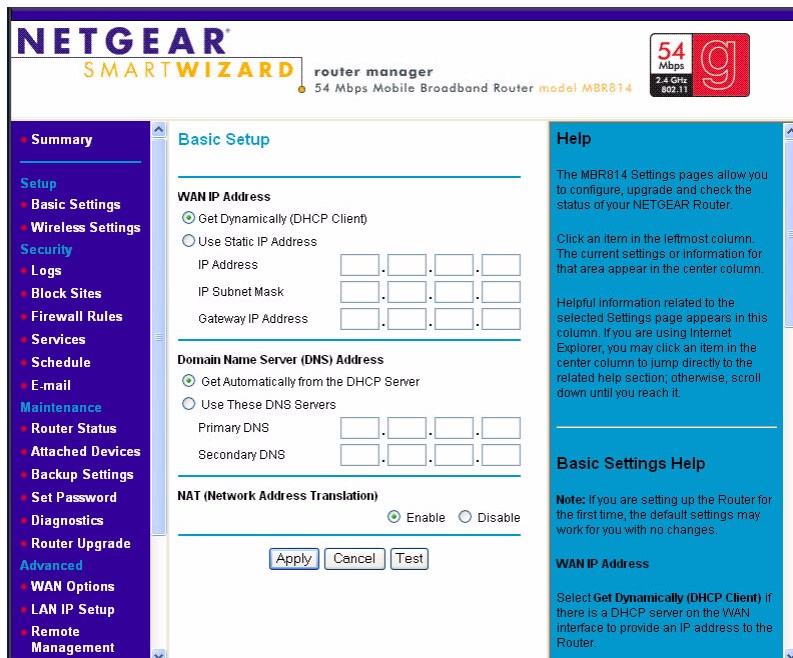


Figure 3-4

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)'.
1. 'WAN IP Address': This section has two radio buttons. The first, 'Get Dynamically (DHCP Client)', is selected. The second, 'Use Static IP Address', is unselected. Below these are three rows of IP address input fields: 'IP Address', 'IP Subnet Mask', and 'Gateway IP Address', each with four boxes for digits and dots.
2. 'Domain Name Server (DNS) Address': This section also has two radio buttons. 'Get Automatically from the DHCP Server' is selected, and 'Use These DNS Servers' is unselected. Below are two rows of DNS input fields: 'Primary DNS' and 'Secondary DNS', each with four boxes for digits and dots.
3. 'NAT (Network Address Translation)': This section has two radio buttons, 'Enable' and 'Disable'. 'Enable' is selected.
At the bottom of the page are three buttons: 'Apply', 'Cancel', and 'Test'.

Figure 3-5

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 MBR814X configuration settings to the factory default. Disable NAT only if you plan to install the MBR814X 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 Mobile Broadband Router MBR814X.

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 the link to [“Wireless Communications:” in Appendix B](#).

To ensure proper compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

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 MBR814X router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

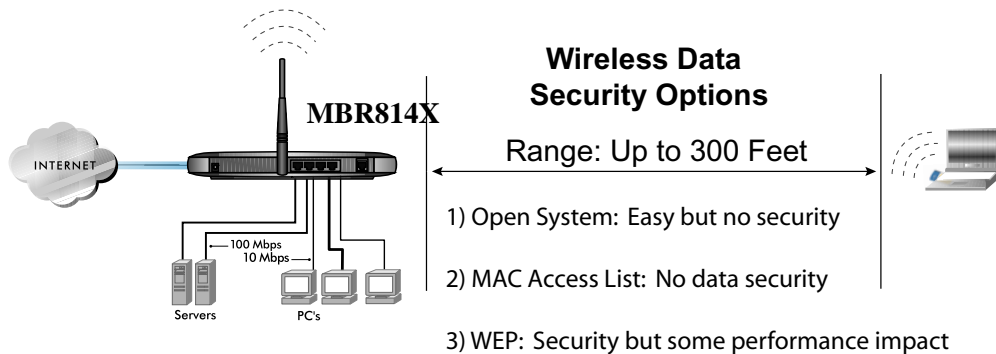


Figure 4-1: MBR814X wireless data security options

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 MBR814X. 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 opens, as shown below:


The screenshot shows the 'Wireless Settings' menu. At the top, the 'Mode' is set to 'g & b'. The 'Wireless Access Point' section has three checkboxes: 'Enable Wireless Access Point' (checked), 'Allow Broadcast of Name (SSID)' (checked), and 'Wireless Isolation' (unchecked). Below this is the 'Wireless Station Access List' section with a 'Setup Access List' button. The 'Security Options' section has four radio buttons: 'Disable', 'WEP (Wired Equivalent Privacy)' (selected), 'WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)', and 'WPA-802.1x'. The 'WEP Security Encryption' section has 'Authentication Type' set to 'Automatic' and 'Encryption Strength' set to '64 bit'. The 'WEP Key' section has a 'Passphrase' field with a 'Generate' button and four key fields: 'Key 1' (selected) with value 'E235485511', 'Key 2' with value '292BB51BCC', 'Key 3' with value '3DCD220BC8', and 'Key 4' with value '97C74DA650'. At the bottom are 'Apply' and 'Cancel' buttons.

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.** Select your region from the drop-down list. This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here.
- **Channel.** This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode.** 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)	<p>You can select the following WEP options:</p> <p>Authentication Type</p> <ul style="list-style-type: none"> • Open: the MBR814X does not perform any authentication. • Shared: WEP shared key authentication. For a full explanation of WEP shared key, see the link to “Wireless Communications:” in Appendix B. <p>Encryption Strength</p> <ul style="list-style-type: none"> • If Shared or Open Network Authentication is enabled, you can choose 64- or 128-bit WEP data encryption. <p>Note: With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the MBR814X <i>does</i> perform 64- or 128-bit data encryption but <i>does not</i> perform any authentication.</p> <p>Security Encryption (WEP) Key</p> <p>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 MBR814X provides two methods for creating WEP encryption keys:</p> <ul style="list-style-type: none"> • 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. <p>Note: Not all wireless adapters support passphrase key generation.</p> <ul style="list-style-type: none"> • Manual. These values <i>are not</i> case sensitive. <ul style="list-style-type: none"> 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).
WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)	<p>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 the link to “Wireless Communications:” in Appendix B.</p> <p>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.</p>

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 MBR814X 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 MBR814X 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 Mobile Broadband Router MBR814X. If they do not match, you will not get a wireless connection to the MBR814X.

4. Set the Region. Select the region in which the wireless interface will operate.
5. Set the Channel. The default channel is 11.

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your firewall. For more information on the wireless channel frequencies please refer to the link to [“Wireless Communications”](#) in Appendix B.

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 Mobile Broadband Router MBR814X 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.

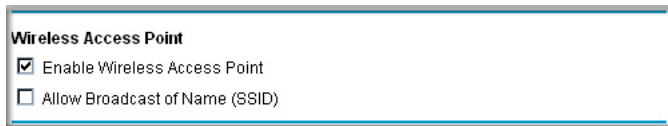



Figure 4-3

Restricting Access to Your Network by Turning Off Wireless Connectivity

You can completely turn off the wireless portion of the MBR814X. 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 MBR814X 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 MBR814X. You must configure your wireless devices to match the wireless network name (SSID) you configure in the MBR814X router.

	Note: The SSID of any wireless access adapters must match the SSID you configure in the Mobile Broadband Router MBR814X. If they do not match, you will not get a wireless connection to the MBR814X.
---	--

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 MBR814X 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:

Wireless Station Access List

Turn Access Control On

Trusted Wireless Stations

Device Name	MAC Address
-------------	-------------

Delete

Available Wireless Stations

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

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 MBR814X. This prevents unauthorized access to your network.

Choosing WEP Authentication and Security Encryption Methods

Security Encryption (WEP)

Authentication Type:

Encryption Strength:

Security Encryption (WEP) Key

Passphrase:

Key 1:

Key 2:

Key 3:

Key 4:

Figure 4-5

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 MBR814X 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 MBR814X router. Please refer to the link to [“Wireless Communications”](#) in Appendix B for a full explanation of each of these options, as defined by the IEEE 802.11g wireless communication standard.

Encryption Choices

Please refer to the link to [“Wireless Communications”](#) in Appendix B 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 MBR814X 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 MBR814X router.
3. Go to the Security Encryption portion of the page:

The screenshot shows the 'Security Encryption (WEP)' configuration interface. It features a dropdown menu for 'Authentication Type' with options: 'Open System', 'Automatic', 'Open System', and 'Shared Key'. Below this is the 'Security Encryption (WEP) Key' section, which includes a 'Passphrase' input field and a 'Generate' button. There are four 'Key' input fields, each with a radio button to its left. 'Key 1' is selected and contains the hexadecimal string 'E18600E9CE520F95AE00B22A'. 'Key 2', 'Key 3', and 'Key 4' are empty. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 4-6

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 MBR814X.

8. 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:

1. 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.
2. Click **Wireless Settings** in the Setup section of the main menu of the MBR814X.
3. Choose the **WPA-PSK** radio button. The WPA-PSK menu will open.
4. Enter the pre-shared key in the Passphrase field.
5. Click **Apply** to save your settings.

Chapter 5

Protecting Your Network

This chapter describes how to use the basic firewall features of the Mobile Broadband Router MBR814X to protect your network.

Protecting Access to Your Mobile Broadband Router MBR814X

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

2. From the main menu of the browser interface, under the Maintenance heading, select Set Password to bring up the Set Password dialog box.

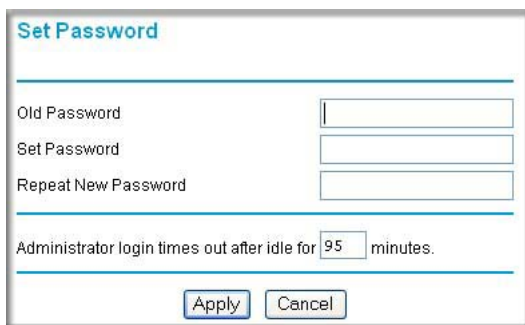


Figure 5-2

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 dialog box, 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 MBR814X 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 MBR814X 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.

Block Sites

Keyword Blocking

Never

Per Schedule

Always

Type Keyword or Domain Name Here.

Add Keyword

Block Sites Containing these Keywords or Domain Names:

Delete Keyword Clear List

Allow Trusted IP Address to Visit Blocked Sites

Trusted IP Address ...

Apply Cancel

Figure 5-3

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 MBR814X 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 MBR814X, 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

- 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 MBR814X 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 below:

The screenshot shows the 'Inbound Services' configuration window. It contains the following fields and values:

- Service:** HTTP(TCP:80)
- Action:** ALLOW always
- Send to LAN Server:** 192 . 168 . 0 . 99
- WAN Users:** Any
- start:** 0 . 0 . 0 . 0
- finish:** 0 . 0 . 0 . 0
- Log:** Never

At the bottom of the window are three buttons: Back, Apply, and Cancel.

Figure 5-5

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' dropdown is set to 'Address Range'. Below it, 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, there are three buttons: 'Back', 'Apply', and 'Cancel'.

Figure 5-6

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 MBR814X 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.

The screenshot shows the 'Outbound Services' configuration window. It has a title bar 'Outbound Services' in blue. Below the title bar, there are several fields: 'Service' is a dropdown menu with 'AIM(TCP:5190)' selected; 'Action' is a dropdown menu with 'BLOCK by schedule, otherwise allow' selected; 'LAN users' is a dropdown menu with 'Any' selected, followed by 'start:' and 'finish:' fields, each with four input boxes for IP address octets; 'WAN Users' is a dropdown menu with 'Any' selected, followed by 'start:' and 'finish:' fields, each with four input boxes for IP address octets; and 'Log' is a dropdown menu with 'Match' selected. At the bottom of the window are three buttons: 'Back', 'Apply', and 'Cancel'.

Figure 5-7

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 Rules table:

Outbound Services							
	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
<input type="radio"/>	1	<input checked="" type="checkbox"/>	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Move"/> <input type="button" value="Delete"/>							
Inbound Services							
	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
<input checked="" type="radio"/>	1	<input checked="" type="checkbox"/>	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
<input type="radio"/>	2	<input checked="" type="checkbox"/>	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Move"/> <input type="button" value="Delete"/>							

Figure 5-8

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 MBR814X 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

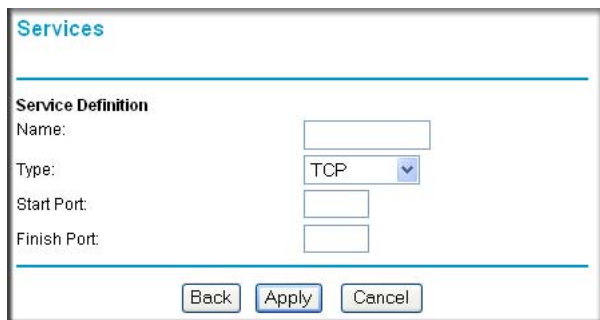
1. Log in to the router at its default LAN address of **http://192.168.0.1** with its default User Name of **admin**, default password of **password**, or using whatever Password and LAN address you have chosen for the router.
2. On the Security menu select the Services link to go to the Service page:



Figure 5-9

- 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 Service Definition page to define or edit a service.



The screenshot shows a web form titled "Services" with a sub-section "Service Definition". The form includes the following fields and controls:

- Name:** A text input field.
- Type:** A dropdown menu currently showing "TCP".
- Start Port:** A text input field.
- Finish Port:** A text input field.

At the bottom of the form, there are three buttons: "Back", "Apply", and "Cancel".

Figure 5-10

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

Setting Times and Scheduling Firewall Services

The MBR814X 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 go to the Schedule page.





Figure 5-11

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.

	<p>Note: If your region uses Daylight Savings Time, you must manually select Adjust for Daylight Savings Time on the first day of Daylight Savings Time, and clear it at the end. Enabling Daylight Savings Time will cause one hour to be added to the standard time.</p>
---	---

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 [Figure 5-11](#).
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 Mobile Broadband Router MBR814X.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the MBR814X 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:

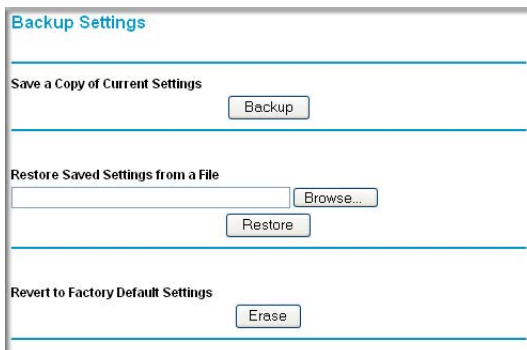


Figure 6-1

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 [“The Router’s Rear Panel”](#) in [Chapter 2](#).

Upgrading the Router’s Firmware

The software of the MBR814X 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 Router Upgrade dialog box:



Figure 6-2

4. Click **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 MBR814X 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 a screen similar to below.

The screenshot displays the 'Router Status' page with the following information:

Router Status	
Firmware Version	V1.3.3
UMTS TD-CDMA	
Modem SW Version	5.2.1.16a
IMEI	351155000056110
Operator	00000
Frequency	2.677GHz
Cell ID	20
Self Test	00000000
WAN Port	
Connection Status	
IP Address	10.10.1.2
DHCP	DHCP Client
IP Subnet Mask	255.255.255.255
Gateway IP Address	10.10.10.1
Domain Name Server	10.10.10.5
	206.13.28.12
	<input type="button" value="Port Status"/>
	<input type="button" value="More Information"/>
LAN Port	
MAC Address	00:0f:b5:c7:f8:8e
IP Address	192.168.0.1
DHCP	On
IP Subnet Mask	255.255.255.0
Wireless Port	
Name (SSID)	WMAN#88e
Region	USA
Channel	11
Wireless AP	enable
Broadcast Name	enable
	<input type="button" value="Show Statistics"/> <input type="button" value="Refresh"/>

Figure 6-3

The Router Status menu provides status and usage information.

This screen shows the following parameters:

Table 6-1. Router Status Fields

Field	Description
Firmware Version	This field displays the router firmware version.
Broadband	These parameters apply to a wireless broadband PC card.
Modem SW Version	Software version used in the broadband PC card.
IMEI	International Mobile Equipment Identity number assigned to the Broadband PC card.
IMSI	International Mobile Subscriber Identity number assigned to the SIM card in the Broadband PC card, if installed.
Operator	Network ISP information.
Frequency	The frequency currently in use for the wireless connection.
Cell ID	The identification number of the cell that the wireless module is currently connected to.
Self Test	The result of the power-on self test.
WAN Port	These parameters apply to the Internet port of the router.
Connection Status	The connection status of the Internet port.
IP Address	The IP address. If no address is shown, the router cannot connect to the Internet.
DHCP	If None, the router uses a fixed IP address on the broadband. If Client, the router gets an IP address dynamically from the ISP.
IP Subnet Mask	The IP Subnet Mask .
Gateway IP Address	The gateway IP address used by the Internet port.
Domain Name Server (DNS)	The DNS Server IP addresses. These addresses are usually obtained dynamically from the ISP.
LAN Port	These parameters apply to the Local (LAN) port of the router.
MAC Address	The Ethernet MAC address.
IP Address	The default IP address 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	The default IP Subnet Mask is 255.255.255.0.
Wireless Port	These parameters apply to the router's wireless connection.
Name (SSID)	Name of the wireless local area network (WLAN).
Region	The country in which the wireless port is configured to operate.
Channel	Current channel in use.
Wireless AP	Indicates if the wireless access point feature is enabled.
Broadcast Name	Indcates if the MBR814X us broadcasting its SSID.

The Router Status page also displays parameter applicable for the broadband module. Please refer to your PC card module for the information regarding the parameters.

Port Status

Click the Port Status button on the Router Status page to display the broadband Status, as shown below:

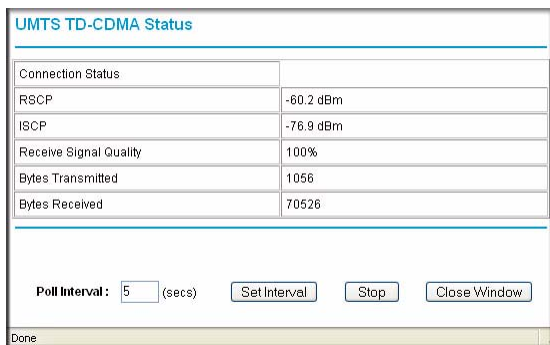


Figure 6-4

Table 6-1. Port Status Fields

Field	Description
Connection Status	The status of the broadband connection.
Receive Signal Quality	The quality of the wireless signal being received by the broadband connection.
Bytes Received	The number of bytes received.
Bytes Transmitted	The number of bytes transmitted

More Information

Click the More Information button on the Router Status page to display more information about the DHCP Client Status.

DHCP Client Status	
IP Address	---
Subnet Mask	---
Default Gateway	---
DHCP Server	---
DNS Server	---
Lease Obtained	---
Lease Time	---

Release Renew

Close Window

Figure 6-5

Clicking the Renew button updates the status information. This screen shows the following statistics:

Table 6-1. More Info Status Fields

Field	Description
IP Address	The IP Address assigned to the WAN port by the Internet Service Provider.
Subnet Mask	The Network Mask assigned to the WAN port by the Internet Service Provider.
Default Gateway	The default gateway router assigned to the WAN port by the 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.

Show Statistics

Click the Show Statistics button on the Router Status page to display router usage statistics, as shown below:

System Up Time 00:29:05

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN (OFDM)	DHCP	36	206	0	2	16	00:28:12
LAN	100M/Full	4323	2939	0	338	201	00:28:53
WLAN	11M/54M	0	0	0	0	0	00:00:00

Poll Interval: (secs)

Figure 6-6

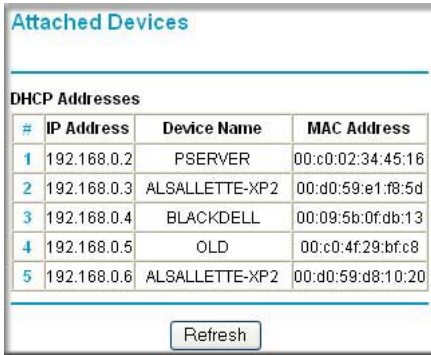
This screen shows the following statistics:

Table 6-1. Show 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.

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 below:



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 6-7

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 6-8

Log entries are described 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 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:

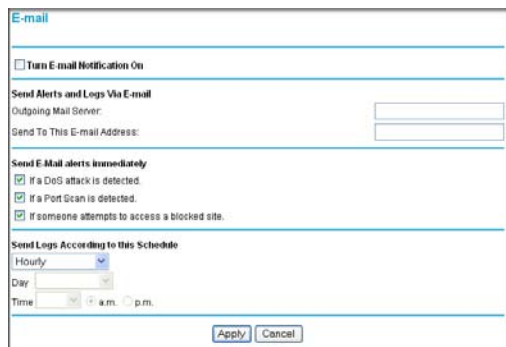


Figure 6-9

- **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.

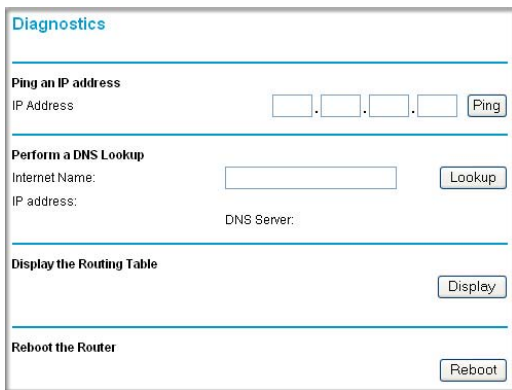
If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, it is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In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

Running Diagnostic Utilities and Rebooting the Router

The MBR814X 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 below:



The screenshot shows a web interface titled "Diagnostics" with four main sections, each separated by a horizontal line:

- Ping an IP address:** Includes a text input field for "IP Address" with four segments separated by dots, and a "Ping" button.
- Perform a DNS Lookup:** Includes a text input field for "Internet Name:", a "Lookup" button, and a "DNS Server:" label with a corresponding text input field.
- Display the Routing Table:** Includes a "Display" button.
- Reboot the Router:** Includes a "Reboot" button.

Figure 6-10

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 Mobile Broadband Router MBR814X.



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 Mobile Broadband Router MBR814X.

Configuring Advanced Security

The Mobile Broadband Router MBR814X 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 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.



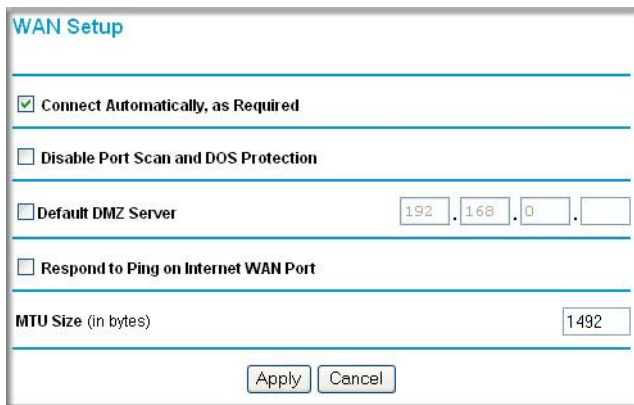
Note: For security reasons, you should avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

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 below:



The screenshot shows the WAN Setup configuration page. The title is "WAN Setup". There are several settings with checkboxes and input fields:

- Connect Automatically, as Required
- Disable Port Scan and DOS Protection
- Default DMZ Server. The IP address field is set to 192.168.0.0.
- Respond to Ping on Internet WAN Port
- MTU Size (in bytes) is set to 1492.

At the bottom of the page are two buttons: "Apply" and "Cancel".

Figure 7-1

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

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 the link to [“Internet Networking and TCP/IP Addressing”](#) in Appendix B 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 go to the LAN IP Setup page:

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

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

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.

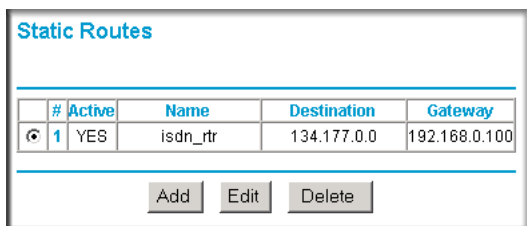
In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like [Figure 7-4](#), below.

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.



#	Active	Name	Destination	Gateway
1	YES	isdn_rtr	134.177.0.0	192.168.0.100

Add Edit Delete

Figure 7-4

3. To add or edit a Static Route:

- a. Click the **Edit** button to open the Edit menu.

Static Routes

Route Name:

Private

Active

Destination IP Address: . . .

IP Subnet Mask: . . .

Gateway IP Address: . . .

Metric:

Figure 7-5

- 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:



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

Figure 7-6

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 Mobile Broadband Router MBR814X. 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 "[Internet Networking and TCP/IP Addressing:](#)" in [Appendix B](#) 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.

Saving Changes

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 broadband connection, then the WAN TCP/IP connection.

Wireless Broadband Link

If your router is unable to access the Internet, you should first determine whether you have broadband wireless coverage in your area. 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 3-8.

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. See the link to [“Internet Networking and TCP/IP Addressing:”](#) in Appendix B. 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 [“Internet Networking and TCP/IP Addressing:”](#) in Appendix B.

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. See the link to [“Internet Networking and TCP/IP Addressing:” in Appendix B](#).
- 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 3-8](#).

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 MBR814X 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 Mobile Broadband Router MBR814X.

Network Protocol and Standards Compatibility

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

Wireless Networking Specifications

Wireless Networking Standard 802.11b

Data rate 1, 2, 5.5, 11Mbps (Auto Rate Sensing)

Signal Frequency 2.4Ghz to 2.5Ghz Direct Sequence Spread Spectrum (DSSS)

Range Depending on various environmental conditions, maximums are:

Outdoor environment	Indoor environment
1Mbps - 1650 ft (503 m)	1Mbps - 500 ft (152 m)
2Mbps - 1320 ft (402 m)	2Mbps - 400 ft (122 m)
5.5Mbps - 1155 ft (352 m)	5.5Mbps - 270 ft (82 m)
11Mbps - 835 ft (255 m)	11Mbps - 175 ft (53 m)

Encryption 64-bit (also called 40-bit) and 128-bit WEP data encryption

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

Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing:	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications:	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access:	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN):	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary:	http://documentation.netgear.com/reference/enu/glossary/index.htm

