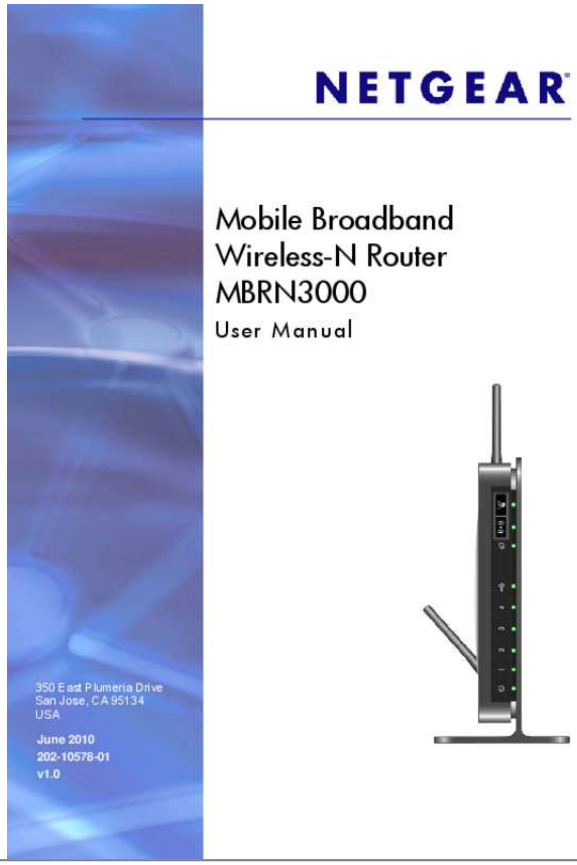

Manual abstract:

0 Technical Support When you register your product at http://www. netgear. @@For other countries, see your Support information card. @@@@Other brand and product names are registered trademarks or trademarks of their respective holders. Statement of Conditions To improve 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. 30 Table of Contents | 3 Mobile Broadband Wireless-N Router MBRN3000 Restoring the Configuration from a File . 60 Testing the Path from Your Computer to a Remote Device . @@@@@@@@The following table lists and describes each LED and button on the front panel of the router. Power is supplied to the router. POST (Power-On Self-Test) failure or device malfunction Power is not supplied to the router Restore Factory Settings Press button for 6 seconds. Power LED lights briefly. When button released, the LED blinks red three times and then turns green as the gateway resets to the factory defaults. Solid green LAN (Ethernet) Blinking green Off Off USB Solid blue Blinking blue Solid green Internet Solid red Blinking green Blinking green and red Off Solid green Wireless Blinking green Off Solid green WPS Blinking green Off Button Description Turn the wireless radio in the router on and off. the wireless radio is on by default. The LED located below this button indicates if the wireless radio is on or off. Wireless Press this button to open a 2-minute window for the router to connect with other WPS-enabled devices. For more information, about using the WPS method to implement security, see â□□Using Push 'N' Connect (WPS) to Configure Your Wireless Networkâ□□ on page 19. The Local port has detected an Ethernet link with a device. Data is being transmitted over the USB port. Data is being transmitted or received over the wireless link. The Wireless Access Point is turned off. WPS wireless security is being enabled. The device is in the 2-minute interval to synchronize security. wPS is not being set or enabled. WPS Chapter 1: Connecting to the Internet | 7 Mobile Broadband Wireless-N Router MBRN3000 Router Back Panel The back panel of the router contains port connections. USB port for Ethernet LAN ports USB docking cable Power On/Off Power adapter input button Figure 2 Back panel Router Label The label on the bottom of the router shows the routerâ□□s MAC address, serial number, security PIN, and factory default login information. restore Factory Settings: Press for 6 seconds. Figure 3 Bottom label 8 | Chapter 1: Connecting to the Internet Mobile Broadband Wireless-N Router MBRN3000 Using the Router Stand You can use the stand to position your router upright. 1.

Insert the tabs of the stand into the slots on the bottom of your router. 2. Place your router near an AC power outlet in a location where you can connect cables as needed for your home network. Logging In to Your Router When you first connect to your router during installation, a Setup Wizard appears. For help using the Setup Wizard to configure your Internet and wireless network, see the Mobile Broadband Wireless-N Router MBRN3000 Installation Guide After the initial configuration, you can use your Web browser to log into the router to view or change its settings. Links to Knowledge Base and documentation are also available on the router main menu. Note: Your computer must be configured for DHCP. For help with configuring DHCP, see the documentation that came with your computer or see the link to the online document in <pdf>â□□Preparing Your Networkâ□□ in Appendix B. When you have logged in, if you do not click Logout, the router waits 5 minutes after no activity before it automatically logs you out. Chapter 1: Connecting to the Internet | 9 Mobile Broadband Wireless-N Router MBRN3000 To log in to the router: 1.

Net in the address field of your browser, and then press Enter. a login window displays: 2. @@For information about how to change the password, see â□□Changing the Built-In Passwordâ□□ on page 23. Note: If you changed your password and do not remember what it is, you can restore the router to its factory settings. If the router has not been configured, the Smart Wizard screen displays.

After the router has been configured, the Firmware Upgrade assistant will appear. â□¢ Checking for Firmware Updates screen. After initial setup, this screen displays unless you have cleared the Check for Updated Firmware Upon Log-in checkbox. â□¢ Router Status screen. The Router Status screen displays if the routerâ□□s Internet connection has not been set up yet.

You can use different methods to configure your router. Â□¢ Select Setup Wizard from the router menu to set up your Internet connection and wireless network configuration. See â□□Accessing the Setup Wizard After Installationâ□□ on page 11. Â□¢ You can manually configure the router settings. see â□□Manually Configuring Your Internet Settingsâ□□ on page 11. 10 | Chapter 1: Connecting to the Internet Mobile Broadband Wireless-N Router MBRN3000 Accessing the Setup Wizard After Installation 1. The Setup Wizard prompts you to set up your Internet connection and wireless network as described in the Mobile Broadband Wireless-N Router MBRN3000 Installation Guide. Manually Configuring Your Internet Settings In order to connect to the network, and active broadband service account is required. Please contact your ISP for user name, password and the network name. Adjust the settings as needed based on your Internet connection.

The fields in this screen are described in Table 2. Depending on your region and ISP, some fields might not be available. 4. The following buttons are available: â□¢ Connect: Manually connect to the network. â□¢ â□¢ â□¢ â□¢ Disconnect: Disconnect from the current network. Apply: Apply the changes that you made. Broadband Settings fields Fields and Checkboxes Username Password PIN code Network name/APN PDP type Connect automatically at startup Description Internet account login username Internet account password for authentication Pin code of the SIM card, where applicable ISP network name Type of packet data protocol If this checkbox is selected, the modem automatically connects to the network when powered up. This should be selected after login information is provided. If this check box is selected, the modem will attempt to reconnect to the network when the connection is lost. Under normal situation, this setting should be selected.

If this checkbox is selected, the unit can roam to any available operator in range and may incur roaming charges. Check with your operator before enabling this feature. Current WAN port status Reconnect automatically when connection is lost Roaming automatically Connection status 12 | Chapter 1: Connecting to the Internet 2.

Wireless Network Configuration 2 For a wireless connection, the SSID, also called the wireless network name, and the wireless security setting must be the same for the router and wireless computers or wireless adapters. nETGEAR strongly recommends that you use wireless security.

Note: Computers can connect wirelessly at a range of several hundred feet. If you do not use wireless security, this can allow others outside of your immediate area to access your network. Planning Your Wireless Network For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly. To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security. Â□¢ To manually configure the wireless settings, you must know the following: SSID.

The default SSID for the router is NETGEAR-3G. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports. see â□□Manually Configuring Your Wireless Settingsâ□□ on page 15. Â□¢ Push 'N' Connect (WPS) implements WPA/WPA2 wireless security on the router and your wireless computer or device at the same time. The wireless computer or device must be compatible with WPS. see â□□Using Push 'N' Connect (WPS) to Configure Your Wireless Networkâ□□ on page 19. Chapter 2: Wireless Network Configuration | 13 Mobile Broadband Wireless-N Router MBRN3000 Wireless Placement and Range Guidelines The range of your wireless connection can vary significantly based on the physical placement of the router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices. For best results, place your router according to the following guidelines: â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ Near the center of the area in which your PCs will operate. In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).

Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage. If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11). 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. Such distances can allow for others outside 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 Mobile Broadband Wireless-N Router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs. 14 | Chapter 2: Wireless Network Configuration Mobile Broadband Wireless-N Router MBRN3000 There are several ways you can enhance the security of your wireless network: Figure 4 Wireless Security â□¢ Restrict Access Based on MAC Address. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the router. 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 â□□discoveryâ□□ feature of some products, such as Windows XP, but the data is still exposed. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. Wi-Fi Protected Access (WPA) with user authentication implemented using IEE 802.

Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise.u will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the router from a wired computer to make further changes. From the main menu, select Wireless Settings to display the Wireless Settings screen. 3. In the Security Options section, select the WEP (Wired Equivalent Privacy) radio button: 4. You can select authentication that requires a shared key, but still leaves data transmissions unencrypted. Security is stronger if you use both the Shared Key and WEP encryption settings. You can manually or automatically program the four data encryption keys.

These values must bed to your router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the routerâ□□s Internet LED blink, indicating communication to the ISP. Note: If no WPS-capable client devices are located during the 2-minute time frame, the SSID does not chnage, and no security is set up. WPS PIN Entry Any wireless computer or device that will connect to the router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart. The first time you add a WPS client, make sure that the Keep Existing Wireless Settings checkbox on the WPS Settings screen is cleared. This is the default setting for the router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the router automatically selects this checkbox so that your SSID and wireless security settings stay the same if other WPS devices are added later. On the router main menu, select Add a WPS Client (computers that will connect wirelessly to the router are clients), and then click Next. Take note of the client PIN.

5. From the router Add WPS Client screen, enter the client PIN number, and then click Next. Â□¢ The router tries to communicate with the client for 4 minutes. If no WPS clients connect during this time, the router wireless settings do not change. Â□¢ The router WPS screen confirms that the client was added to the wireless network.

Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See â□□Manually Configuring Your Wireless Settingsâ□□ on page 15 To access the Internet from any computer connected to your router, launch an Internet browser such as Mozilla Firefox.

You should see the routerâ□□s Internet LED blink Chapter 2: Wireless Network Configuration | 21 Mobile Broadband Wireless-N Router MBRN3000 Adding Wireless Computers that Do Not Support WPS If you set up your network with WPS, and now you want to add a computer that does not support WPS, you must manually configure that computer. To view the wireless settings for the router, see â□□Manually Configuring Your Wireless Settingsâ□□ on page 15.

Because WPA randomly creates the SSID and WPA/WPA2 keys, they might be difficult to type or remember (that is one reason why the network is so secure). You can change the wireless settings so that they are easier for you to remember. If you do that, then you will need to set up the WPS-compatible computers again. Changing Wireless Settings for the Network: Note: Making these changes will cause all wireless computers to be disconnected from network. You will then have to set them up with the new wireless settings. 1. Use an Ethernet cable to connect a computer to the router. That way you will not get disconnected when you change the wireless settings. Make the following changes: â□¢ Change the Wireless Network Name (SSID) to a meaningful name. â□¢ â□¢ On the WPA/PSK + WPA2/PSK screen , select a passphrase.

Make sure that the Keep Wireless Settings checkbox is selected in the WPS Settings screen so that your new settings will not be erased if you use WPS. 4. Click Apply so that your changes take effect. Write down your settings. All existing wireless clients are disassociated and disconnected from the router. 5. For the non-WPS devices that you want to connect, open the networking utility and follow the utilityâ□□s instructions to enter the security settings that you selected in Step 2 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase). 6. For the WPS devices that you want to connect, follow the procedure â□□WPS Buttonâ□□ on page 20 or â□□WPS PIN Entryâ□□ on page 21. The settings that you configured in Step 2 are broadcast to the WPS devices so that they can connect to the router.

22 | Chapter 2: Wireless Network Configuration 3. Protecting Your Network 3 This chapter describes how to use the basic firewall features of the router to protect your network. Note: For information about the advanced content filtering features port forwarding and port triggering, see â□□Port Forwarding and Port Triggeringâ□□ on page 46. Protecting Access to Your Mobile Broadband Wireless-N Router For security reasons, the router has its own user name and password. Also, after a period of inactivity, the login automatically disconnects.

The user name and password are not the same as a user name or password you might 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. changing the Built-In Password 1.

To log in to the router, type http://www. routerlogin. Net in the address field of your Internet browser. @@Note: If you changed the password and do not remember what it is, you can reset the router to its factory default settings. From the main menu, under the Maintenance heading, select Set Password: 3. To change the password, first enter the old password, and then enter the new password twice. Note: After changing the password, you must 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 Time-out For security, the administrator login to the router configuration times out after a period of inactivity. to change the login time-out period: 1.

In the Set Password screen, type a number in the Administrator login times out field. Click Apply to save your changes, or click Cancel to keep the current period. blocking Sites and Keywords The router provides a variety of options for blocking Internet-based content and communications services. With its content filtering feature, the router prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for keywords within Web addresses. Limits access from your LAN to Internet locations or services that you specify as off-limits. 24 | Chapter 3: Protecting Your Network Mobile Broadband Wireless-N Router MBRN3000 â□¢ Blocking unwanted traffic from the Internet to your LAN. The router allows you to restrict access to Internet content based on Web addresses and Web address keywords. On the main menu, select Block Sites to display the Block Sites screen: 3. to enable keyword blocking , select one of the following: â□¢ Per Schedule.

Turn on keyword blocking according to the settings on the Schedule screen. â□¢ Always. Turn on keyword blocking all the time, independent of the setting in the Schedule screen. 4. Enter a keyword or domain in the Keyword field, click Add Keyword, and then click Apply.

Some examples of keyword applications are shown in the following chart. Only websites with other domain suffixes (such as . Up to 32 entries are supported in the Keyword list. Note: If you block sites, you can set up the router to log attempts to access them. To delete a keyword or domain, select it from the list, click Delete Keyword, and then click Apply.

6. To specify a trusted user, enter that computerâ□□s IP address in the Trusted IP Address field, and then 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. In the main menu, under Content Filtering, select Block Services to display this screen: . Turn on keyword blocking according to the settings in the Schedule screen. â□¢ Always. Turn on keyword blocking all the time, independent of the Schedule screen. Either select a service from the Service Type drop-down list, or use the Service/Type User Defined field to create a custom service. 6.

Click Add to create the service, and it will be listed in the Service Table on the Block Services screen. Scheduling The router uses network time protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet. Setting Your Time Zone To localize the time for your log entries, you must specify your time zone: 1. On the main menu below Content Filtering, select Schedule: 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. If your time zone is currently in daylight savings time, select the Automatically adjust for daylight savings time check box.

Scheduling Firewall Services If you enabled services blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted. On the main menu, select the Schedule. 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, fill in the Start Blocking and End Blocking fields. 4. Enter the values in 24-hour time format. Would be 10 hours and 30 minutes, and 10:30 p.

m. 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. Live Parental Controls is an excellent solution for keeping your family safe online, but like all Web filtering tools, it isn't perfect. NETGEAR reminds you thereâ□□s no substitute for keeping the family computer in a common area and in plain sight where you can monitor the websites your kids are visiting, and taking caution when visiting Web sites requesting personal or financial information.

To download Live Parental Controls, click the Live Parental Controls link on the router menu to go to the website: http://www. Web-based GUI Live Parental Controls is the first to allow parents or network administrators to manage settings while away from home or office. This is particularly convenient when access â□□exceptionsâ□□ need to be made. And since settings are stored on the web, using a browser interface to manage them is not difficult at all. Total home protection Live Parental Controls protects all Internet-connected devices thru the router. It not only protects computers, but also set-top boxes, iPhones, iPods, and gaming consoles that are attached to your network. You no longer need to worry about phones and gaming consoles not being protected when kids use them in their own rooms. Even guest computers accessing the Internet through your network are protected. Flexible settings You may have your own computer or you may be sharing a computer with other members in the family. Default and per-user settings allow customizable configurations for different computing arrangement and personalize the settings for each person.

Per-time setting allows Internet access during scheduled time slots, to help manage work/play balance. minimal software installation Installation requires a one-time installation of the Management Utility. Once Live Parental Controls is set up, the software runs in the background and does not interfere with normal Internet usage. chapter 3: Protecting Your Network | 29 4. Managing Your Network 4 This chapter describes how to perform network management tasks with your Mobile Broadband Wireless-N Router. Backing Up, Restoring, or Erasing Your Settings The configuration settings of the 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. Net in the address field of your Internet browser. @@ 2.

Under the Maintenance heading on the main menu, select Backup Settings to display the Backup Settings screen: 3. Click Save to save a copy of the current settings. Chapter 4: Managing Your Network | 30 Mobile Broadband Wireless-N Router MBRN3000 Restoring the Configuration from a File To restore the configuration: 1. Net in the address field of your Internet browser. @@ 2.

Under the Maintenance heading on the main menu, select Backup Settings. 3. Enter the full path to the file on your network, or click Browse to locate the file. 4. When you have located the .

Cfg file, click Restore to upload the file to the router. Erasing the Configuration You can use the Erase feature to erase its configuration settings and restore the router to the factory default settings. to erase the configuration: 1. Under the Maintenance heading on the main menu select, Backup Settings. After an erase, the router password is password, the LAN IP address is 192. Note: To restore the factory default configuration settings when you do not know the login password or IP address, press the Restore Factory Settings button on the bottom of the router for 6 seconds. Upgrading the Router Firmware The router firmware is stored in flash memory, and can be upgraded as new firmware is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR website. if the upgrade file is compressed (a . Zip file), you must first extract the binary (.

bin or . Img) file before uploading it to the router. NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you might need to restore your configuration settings. 1. Download and unzip the new firmware file from NETGEAR. Chapter 4: Managing Your Network | 31 Mobile Broadband Wireless-N Router MBRN3000 The Web browser used to upload new firmware into the router must support HTTP uploads. Net in the address field of your Internet browser. @@ 3. From the main menu, under the Maintenance heading, select Router Upgrade to display this screen: 4.

When uploading firmware to the router, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it might corrupt the firmware, causing router to be unworkable and inaccessible. When the upload is complete, your router will automatically restart. The upgrade process typically takes about 1 minute. In some cases, you might need to clear the configuration and reconfigure the router after upgrading.

32 | Chapter 4: Managing Your Network Mobile Broadband Wireless-N Router MBRN3000 Router Status From the main menu, below the Maintenance heading, select Router Status to view this screen. You can use this screen to view the status of the router, to show statistics, or to view the connection status. Â□¢ â□¢ â□¢ For information about the fields on this screen, see Table 4. See â□□Showing Statisticsâ□□ on page 35 for information about statistics. For information about the Internet connection, see â□□Connection Statusâ□□ on page 36 Table 4.

Router Status Fields Field Firmware Version HSDPA (High-Speed Downlink Packet Access) Modem Identity Modem sw version Modem driver version IMSI IMEI Operator Network mode Description This field displays the router firmware version. shows the modem in use. The software version of the modem. The driver version of the modem. The ISP for the broadband wireless network. The mode of the current network the modem is connected to. This is dependent on coverage and distance from the cell site. The IP address used by the modem. If no address is shown, the router cannot connect to the Internet. The protocol for the Internet connection, which is PPP (Point-to-Point).

The IP subnet mask used by the routerâ□□s USB port.

Gateway IP Address The IP address used by the router. Domain Name Server LAN Port MAC Address IP Address DHCP The DNS server IP addresses used by the router. These addresses are usually obtained dynamically from the ISP. The Ethernet MAC address used by the routerâ□□s LAN port. Â□¢ Off: The router will not assign IP addresses to PCs on the LAN. The service set ID, also known as the wireless network name. The country where the unit is set up for use. The current channel, which determines the operating frequency. indicates if the access point feature is disabled or not.

If not enabled, the Wireless LED on the front panel will be off. Indicates if the router is configured to broadcast its SSID. iP Subnet Mask Wireless Port (See â□□Manually Configuring Your Wireless Settingsâ□□ on page 15. Name (SSID) Region Channel Wireless AP Broadcast Name 34 | Chapter 4: Managing Your Network Mobile Broadband Wireless-N Router MBRN3000 Showing Statistics Click the Show Statistics button on the Router Status screen to display router usage statistics: This following table explains the statistic fields. Note that LAN2, LAN3, and LAN4 are guest networks.

The number of packets transmitted on this port since reset or manual clear. The number of packets received on this port since reset or manual clear. The number of collisions on this port since reset or manual clear. The average egress line utilization for this port. The average ingress line utilization for this port. The time elapsed since the last power cycle or reset. Chapter 4: Managing Your Network | 35 Mobile Broadband Wireless-N Router MBRN3000 Connection Status Click the Connection Status button on the Router Status screen: This screen shows the following statistics: Table 6. Connection Status Fields for HSDPA Status Field Connection Status Description The status of the Internet connection. â□¢ Scanning. The modem is scanning for broadband wireless networks in your area. â□¢ Connected. The router is connected to the Internet. â□¢ No USB Device Attached. The router does not detect a USB modem connected to its USB port. Either the modem is disconnected, or it is not correctly seated.

To correct the problem remove the modem and reinsert it into the port. modem radio reception. A small, negative number indicates good signal quality. The number of bytes transmitted in the most recent connection session. The number of bytes received in the most recent connection session. Time elapsed since the last reboot. The time elapsed since the most recent connection to the Internet. The broadband wireless networks available in your area. Received Signal Quality (in dbm) Bytes Transmitted Bytes Received Tx B/s Rx B/s System Uptime Connection Duration Available Networks 36 | Chapter 4: Managing Your Network Mobile Broadband Wireless-N Router MBRN3000 Viewing Attached Devices The Attached Devices screen shows all IP devices that the router discovered on the local network. From the main menu, under the Maintenance heading, select Attached Devices: For each device, the table shows the IP address, device name if available, and the Ethernet MAC address.

If the router is rebooted, this 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 logs security-related events such as denied incoming service requests , hacker probes , and administrator logins. If you enabled content filtering in the Block Sites screen, the Logs screen can show you when someone on your network tries to access a blocked site. On the router menu, below the Content Filtering heading, select Logs to display this screen: Note: You can enable e-mail notification to receive these logs in an e-mail message.

see â□□Enabling Security Event E-mail Notificationâ□□ on page 39. Chapter 4: Managing Your Network | 37 Mobile Broadband Wireless-N Router MBRN3000 Log entries and action buttons are described in the following table. table 7. Security Log Entry and Button Descriptions Field or button Current time Description or action Source IP Source port and interface Destination Destination port and interface Refresh button Clear Log button Send Log button Apply button Cancel button Description The date and time the log entry was recorded. The type of event and what action was taken if any.

The IP address of the initiating device for this log entry. The service port number of the initiating device, and whether it originated from the LAN or WAN. The name or IP address of the destination device or website. The service port number of the destination device, and whether it is on the LAN or WAN. Selecting Which Information to Log Besides the standard information listed previously, you can choose to log additional information. Those optional selections are as follows: â□¢ â□¢ â□¢ â□¢ Attempted access to blocked site Connections to the router menu Router operation (start up, get time, and so on) 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 the Broadcast on LAN radio button 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. 38 | Chapter 4: Managing Your Network Mobile Broadband Wireless-N Router MBRN3000 Activation and Administration Tue, 2002-05-21 18:48:39 - NETGEAR activated [This entry indicates a power-up or reboot with initial time entry.

2 [This entry shows an administrator logging in and out from IP address 192. 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 e-mailed. 11,21,LAN - [Inbound Default rule match] Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64. 11,6970,LAN - [Inbound Default rule match] Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64. 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 To set up the router so that you can receive logs and alerts by e-mail, select Email from the router menu to display the following screen: Chapter 4: Managing Your Network | 39 Mobile Broadband Wireless-N Router MBRN3000 To receive alerts and logs by e-mail: 1. Fill in the fields to send alerts and logs through email. â□¢ Your Outgoing Mail Server. Enter the name or IP address of the outgoing SMTP mail server of your ISP (such as mail.

Enter the e-mail address where you want to send the alerts and logs.

Use a full e-mail address, such as ChrisXY@myISP. Select this check box if you need to log in to your SMTP server to send E-mail. If you select this feature, you must enter the user name and password for the mail server. Tip: If you cannot remember this information, check the settings in your email program. 3. Specify when you want the alerts and logs to be sent: â□¢ 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. Â□¢ 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. 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 routerâ□□s memory. If the router cannot e-mail the log file, the log buffer might fill up. @@ 4.

Click Apply so that your changes take effect. @@@@@@@@@@@@@@@@ display: View the internal routing table. Typically, this information is used only by Technical Support. Reboot: Shut down and restart the router. @@@@ â□¢ â□¢ Save: Save diagnostic information. @@@@@@Your password can be up to 30 characters. Net in the address field of your Internet browser. @@ 2. Under the Advanced heading, select Remote Management: 3. @@@@@@Enter a beginning and ending IP address to define the allowed range.

@@Enter the IP address that will be allowed access. â□¢ 5. @@ access normally uses the standard HTTP service port 80. For greater security, you can enter a different port number. @@The default is 8080, which is a common alternate for HTTP.

6. Click Apply to have your changes take effect. @@For example, if your external address is 134. 123 and you use port number 8080, enter: http://134. @@ 42 | Chapter 4: Managing Your Network 5.

@@@@@@@@These should be left at their default settings. @@@@By default, this check box is cleared. This allows the WPS clients to discover the routerâ□□s PIN. By default, this check box is cleared. @@@@@@ see Restricting Access by MAC Address. @@You can use Wireless Access Point settings in the Wireless Setting screen to further restrict wireless access to your network: â□¢ Turning off wireless connectivity completely. You can completely turn off the wireless portion of the router. For example, if you use your notebook computer 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 can still use the router. To do this, clear the Enable Wireless Access Point check box on the Wireless Settings screen, and then click Apply.

hiding your wireless network name (SSID). By default, the router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To do this, clear the Allow Broadcast of Name (SSID) check box on the Wireless Settings screen, and then click Apply. Wireless devices will not â□□seeâ□□ your router. You must configure your wireless devices to match the wireless network name (SSID) of the router. Â□¢ Note: The SSID of any wireless access adapters must match the SSID you configure in the router. If they do not match, you will not get a wireless connection to the router. 44 | Chapter 5: Advanced Mobile Broadband Wireless-N Router MBRN3000 Restricting Access by MAC Address For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the Mobile Broadband Wireless-N Router.

MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. To restrict access based on MAC addresses: Note: If you configure the router from a wireless computer, add your computerâ□□s MAC address to the access list. Otherwise you will lose your wireless connection when you click Apply. You must then access the router from a wireless computer that is on the access control list, to make any further changes. 1.

From the main menu, below the Advanced heading, select Wireless Settings. Adjust the list as needed for your network. You can add devices to the Trusted Wireless Stations list. click Add to display the following screen: 3. You can add devices to the list using either of the following methods: â□¢ If the computer is in the Available Wireless Cards table, select its radio button to capture its MAC address.

Â□¢ â□¢ Use the Wireless Card Entry fields to enter the MAC address of the device to be added. The MAC address can usually be found on the bottom of the wireless device. If no device name appears when you enter the MAC address, you can type a descriptive name for the computer that you are adding. Now, only devices on this list will be allowed to wirelessly connect to the router. @@@@@@ port triggering monitors outbound traffic. @@@@@@@@@@ 2. You can select a service or create a custom service. @@Fill in the fields in the Add Custom Service screen. The service appears in the list. @@@@ 2.

Select the Port Triggering radio button to display the following screen: 3. Click Add Service and fill in the fields in the Add Service screen. The service appears in the list. For more detailed information, see the Port Forwarding/Port Triggering help. wAN Setup To change broadband Internet connection settings , use the Broadband Settings screen , as described in â□□Manually Configuring Your Internet Settingsâ□□ on page 11. To view or change the WAN Setup: 1. From the main menu, select WAN Setup to display the WAN Setup screen: 2. Make the changes that you want, and then click Apply to save the settings. The WAN Setup fields are described in the following table. chapter 5: Advanced | 47 Mobile Broadband Wireless-N Router MBRN3000 Table 9. WAN Setup Settings Setting Disable SPI Firewall Description This check box is usually clear so that the firewall protects your LAN against port scans and denial of service (DOS) attacks. This check box should be selected only in special circumstances. This feature is sometimes helpful when you are using some online games and videoconferencing. Be careful when using this feature because it makes the firewall security less effective. see â□□Setting Up a Default DMZ Serverâ□□ on page 48.

If you want the router to respond to a ping from the Internet, select this check box.

This should be used only as a diagnostic tool, since it allows your router to be discovered. Do not select this check box unless you have a specific reason to do so. maximum Transmit Unit (MTU) value. For most Ethernet networks this is 1500 bytes, or 1492 bytes for PPPoE connections, or 1436 bytes for PPTP connections.

This is set to Secured to provide a secure firewall to protect computers on the LAN from attacks from the Internet. The Open setting is less secure. Some VoIP applications do not work well with SIP ALG. Selecting this check box might help your VoIP devices create or accept a call through the router. default DMZ Server Respond to Ping on Internet MTU Size NAT Filtering Disable SIP Alg Setting Up a Default DMZ Server WARNING! 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. The default DMZ server feature is helpful when you are 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 computerâ□□s IP address is entered as the default DMZ server.

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 screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server. 48 | Chapter 5: Advanced Mobile Broadband Wireless-N Router MBRN3000 To assign a computer or server to be a default DMZ server: 1. Go to the WAN Setup screen as described in the previous section. Type the IP address for that server. These features can be found under the Advanced heading in the router main menu. The router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. 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 screen.

To view or change the LAN IP Setup: Tip: If you change the LAN IP address of the router while connected through the browser, you will be disconnected and so will others connected to the router. To connect to the router, you must open a new connection to the new IP address and log in again. Others using the router must restart their computers to connect to the router again. For more information, see Table 10, â□□DHCP Settingsâ□□ on page 50 or â□□Reserved IP Addressesâ□□ on page 51. The LAN TCP/IP Setup parameters are explained in the following table.

chapter 5: Advanced | 49 Mobile Broadband Wireless-N Router MBRN3000 Table 10. LAN IP Setup Settings Device Name LAN TCP/IP Setup IP Address IP Subnet Mask Description The LAN IP address of the router. 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. This check box is usually selected so that the router functions as a Dynamic Host Configuration Protocol (DHCP) server.

see â□□DHCP Settingsâ□□ on page 50. Specify the start of the range for the pool of IP addresses in the same subnet as the router. Specify the end of the range for the pool of IP addresses in the same subnet as the router. Use Router as a DHCP DHCP Server Server For more information, see â□□DHCP Starting IP Address Settingsâ□□ on page 50. Ending IP Address Address Reservation When you specify a reserved IP address for a computer on the LAN, For more information, see â□□DHCP Settingsâ□□ that computer receives the same IP address each time it access the on page 50. DHCP Settings By default, the router functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the routerâ□□s LAN. The assigned default gateway address is the LAN address of the router. IP addresses is assigned to the attached PCs from a pool of addresses specified in this screen. 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 online document listed in "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 on the LAN IP Setup screen. Otherwise, leave it selected. Specify the pool of IP addresses to be assigned by filling in the Starting IP Address and Ending IP Address fields. These addresses should be part of the same IP address subnet as the routerâ□□s LAN IP address. Using the default addressing scheme, you should define a range between 192. 254, although you might want to save part of the range for devices with fixed addresses. 50 | Chapter 5: Advanced Mobile Broadband Wireless-N Router MBRN3000 The router delivers the following parameters to any LAN device that requests DHCP: â□¢ â□¢ â□¢ â□¢ â□¢ An IP address from the range you have defined. Primary DNS server, if you entered a primary DNS address in the Basic Settings screen; otherwise, the routerâ□□s LAN IP address. Secondary DNS server, if you entered a secondary DNS address in the Basic Settings screen.

WINS Server (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 serverâ□□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 always receives the same IP address each time it access the routerâ□□s DHCP server.

Reserved IP addresses should be assigned to servers that require permanent IP settings. In the IP Address field, type the IP address to assign to the computer or server. Choose an IP address from the routerâ□□s LAN subnet, such as 192.

Type the MAC address of the computer or server. Tip: If the computer is on your network, it is listed on the same page for your convenience. Clicking the radio button for each entry in the attached device list fills in the fields automatically with the computerâ□□s MAC address and name. 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 routerâ□□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. Chapter 5: Advanced | 51 Mobile Broadband Wireless-N Router MBRN3000 Dynamic DNS If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service to register your domain to their IP address, and forward traffic directed at your domain to your frequently changing IP address.

The router contains a client that can connect to a Dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the router, whenever your ISP-assigned IP address changes, your router will automatically contact your Dynamic DNS service provider, log in to your account, and register your new IP address. configuring Dynamic DNS WARNING! If your ISP assigns a private WAN IP address such as 192. X, the Dynamic DNS service will not work because private addresses will not be routed on the Internet. 1. From the main menu, select Dynamic DNS to display the Dynamic DNS screen: 2. Access the website of one of the Dynamic DNS service providers whose names appear in the Service Provider drop-down list, and register for an account. For example, for dyndns. Select the name of your dynamic DNS service provider.
5. Fill in the Host Name, User Name, and Password fields. The dynamic DNS service provider may call the host name a domain name. The password can be a key for your dynamic DNS account. 52 | Chapter 5: Advanced Mobile Broadband Wireless-N Router MBRN3000 6.
*If your dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the Use wildcards check box to activate this feature. For example, the wildcard feature will cause *. Org to be aliased to the same IP address as yourhost. 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: â□¢ â□¢ â□¢ 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 routerâ□□s address on your LAN is 192. 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. With this configuration, if you attempt to access a device on the 134. 0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the companyâ□□s firewall. In this case you must define a static route, telling your router that 134.

0 should be accessed through the ISDN router at 192. In this example: â□¢ â□¢ â□¢ The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134. The Gateway IP Address fields specify that all traffic for these addresses should be forwarded to the ISDN router at 192. In the Metric field, a 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. â□¢ Chapter 5: Advanced | 53 Mobile Broadband Wireless-N Router MBRN3000 To configure static routes: 1. From the main menu, under the Advanced heading, select Static Routes to view the Static Routes screen: 2. click Add or Edit to display the following screen: 3.
Fill in or change the fields: â□¢ Route Name. The route name is for identification purposes only. â□¢ â□¢ â□¢ â□¢ â□¢ Private. Select this check box if you want to limit access to the LAN only. The static route will not be reported in RIP.
active. Select this check box to make this route effective. destination IP Address , and IP Subnet Mask. If the destination is a single host, type a subnet value of 255. This must be a router on the same LAN segment as the router.
metric. Type a number between 2 and 15. 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 2. 4. Click Apply to either save your changes. If you added a static route, it is added to the Static Routes screen. 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. 54 | Chapter 5: Advanced Mobile Broadband Wireless-N Router MBRN3000 1.

Select UPnP on the main menu to display the UPnP screen: 2. Fill in the settings on the UPnP screen: â□¢ 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. â□¢ Advertisement Period. The advertisement period is how often the router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is for 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic.
Longer durations might 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 might 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. â□¢ â□¢ 3. To save, cancel your changes, or refresh the table: â□¢ Click Apply to save the new settings to the router. â□¢ â□¢ Click Cancel to disregard any unsaved changes. Click Refresh to update the portmap table and to show the active ports that are currently opened by UPnP devices. Traffic Meter Traffic Metering allows you to monitor the volume of Internet traffic passing through your routerâ□□s Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage. chapter 5: Advanced | 55 Mobile Broadband Wireless-N Router MBRN3000 To monitor traffic on your router: 1. Under the Advanced heading on the router menu, select Traffic Meter. 2. To enable the Traffic Meter, select the Enable Traffic Meter check box. 3.

If you would like to record and restrict the volume of Internet traffic, select the Traffic volume control by radio button. You can select one of the following options for controlling the traffic volume: â□¢ No Limit. The restriction is applied to both incoming and outgoing traffic. 4. You can limit the amount of data traffic allowed per month: â□¢ By specifying how many Mbytes per month are allowed. Â□¢ By specifying how many hours of traffic are allowed. 5. Set the Traffic Counter to begin at a specific time and date. 6. Set up Traffic Control to issue a warning message before the month limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained: â□¢ The Internet LED flashes green or amber. Click the Traffic Status button if you want a live update on Internet traffic status on your router. Troubleshooting 6 This chapter gives information about troubleshooting your Mobile Broadband Wireless-N Router. 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. â□¢ â□¢ Is the router on? Have I connected the router correctly? go to â□□Basic Functioningâ□□ on page 57. Â□¢ I canâ□□t access the routerâ□□s configuration with my browser. go to â□□Troubleshooting Access to the Router Main Menuâ□□ on page 58. Â□¢ Iâ□□ve configured the router but I canâ□□t access the Internet. 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 2. After approximately 10 seconds, verify that: a. the Power LED is still solid green. A red light indicates the unit has failed its power-on self-test (POST). b. The Ethernet LAN port LEDs are lit for any local ports that are connected. If the port is 10 Mbps, the LED is amber. c. The USB and Internet LEDs are lit. lED is on.

Chapter 6: Troubleshooting | 57 Mobile Broadband Wireless-N Router MBRN3000 If any of these conditions does not occur, refer to the following table. Action â□¢ Make sure that the power cord is properly connected to your â□¢ â□¢ router and that the power supply adapter is properly connected to a functioning power outlet. Check that you are using the power adapter supplied by NETGEAR for this product. If the error persists, you have a hardware problem and should contact technical support. Power LED is red There is a fault within the router. Try to clear the fault as follows: â□¢ Cycle the power to see if the router recovers. Â□¢ Clear the routerâ□□s configuration to factory defaults. This sets the routerâ□□s IP address to 192. This procedure is explained in â□□Restoring the Default Configuration and Passwordâ□□ on page 62. If the error persists, you might have a hardware problem and should contact technical support. The router cannot connect to the Internet. Â□¢ Make sure the USB LED is lit, indicating that the wireless modem is securely connected to the router. Â□¢ Your wireless modem must be activated and there must be coverage in your area. To test coverage, connect your modem to your PC, and try to connect to the Internet directly from your computer. Â□¢ Check the NETGEAR website to ensure that your wireless modem is supported. Â□¢ Close the 3G Connection manager if it is running on your PC. If these LEDs do not light when the Ethernet connection is made, check the following: â□¢ Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation. Â□¢ Make sure that power is turned on to the connected hub or workstation. The traffic meter feature is enabled and the limit set has been reached. Internet LED is blinking red and green Troubleshooting Access to the Router Main Menu If you are unable to access the router main menu from a computer on your local network, check the following: â□¢ If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section. 58 | Chapter 6: Troubleshooting Mobile Broadband Wireless-N Router MBRN3000 â□¢ Make sure your computerâ□□s IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computerâ□□s address should be in the range of 192. See the online document listed in "Internet Networking and TCP/IP Addressing: " in Appendix B to find your computerâ□□s IP address. Note: If your computerâ□□s IP address is shown as 169. X: Recent versions of Windows and MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer. Â□¢ If your routerâ□□s IP address was changed and you do not know the current IP address, clear the routerâ□□s configuration to factory defaults. This will set the routerâ□□s IP address to 192. This procedure is explained in â□□Restoring the Default Configuration and Passwordâ□□ on page 62.

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