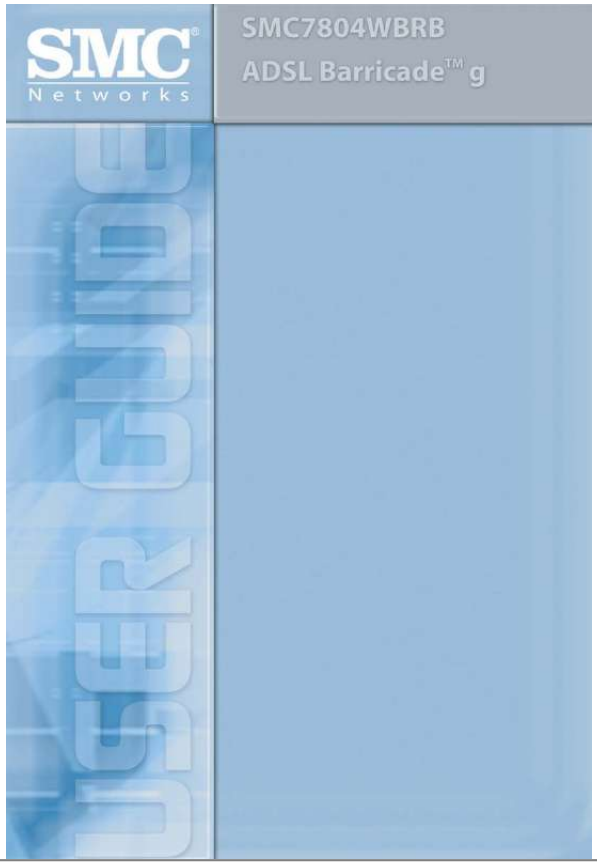

Manual abstract:

38 Tesla Irvine, CA 92618 All rights reserved. Trademarks: SMC is a registered trademark; and Barricade is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders. LIMITED WARRANTY Limited Warranty Statement: SMC Networks, Inc. ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product. The standard limited warranty can be upgraded to a Limited Lifetime warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site.*

Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product. A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product.

A list of discontinued products with their respective dates of discontinuance can be found at:

http://www.smc.com/index.cfm?action=customer_service_warranty. All products that are replaced become the property of SMC.

Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product. Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC.

*SMC is responsible for return shipping charges from SMC to customer. i LIMITED WARRANTY WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD. LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS. * SMC will provide warranty service for one year following discontinuance from the active SMC price list.*

Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase. SMC Networks, Inc. 38 Tesla Irvine, CA 92618 ii COMPLIANCES Federal Communication Commission Interference 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 instructions, may cause harmful interference to radio communications.

However, there is no guarantee that the 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 FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. 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.

IMPORTANT STATEMENT FCC Radiation Exposure Statement This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 cm (8 in) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. FCC - Part 68 This equipment complies with Part 68 of the FCC rules. This equipment comes with a label attached to it that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company. This equipment uses the following USOC jacks: RJ-11C. iii COMPLIANCES The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0).

To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum REN for the calling area. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary. The telephone company may make changes in its facilities, equipment, operations, or procedures that will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service. If trouble is experienced with this equipment, please contact our company at the numbers shown on back of this manual for repair and warranty information. If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved. No repairs may be done by the customer. This equipment cannot be used on telephone company-provided coin service. Connection to Party Line Service is subject to state tariffs.

When programming and/or making test calls to emergency numbers: · Remain on the line and briefly explain to the dispatcher the reason for the call. · Perform such activities in off-peak hours such as early morning or late evenings. The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device to send any message via a telephone facsimile machine unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or such business, other entity, or individual. In order to program this information into your facsimile, refer to your communications software user manual. Industry Canada - Class B This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matérial brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie. iv COMPLIANCES Australia AS/NZS 3548 (1995) - Class B ACN 096 592 442 SMC contact for products in Australia is: SMC-Australia L9, 123 Epping Rd., North Ryde, NSW Australia Phone: 61-2-88757887 Fax: 61-2-88757777 EC Conformance Declaration The following importer/manufacturer is responsible for making this declaration: SMC Networks Europe, Edificio Conata II, Calle Fructuós Gelabert 6-8, 2o, 4a, 08970 - Sant Joan Despí, Barcelona, Spain. This RF product complies with R&TTE Directive 99/5/EC. For the evaluation of the compliance with this Directive, the following standards were applied: · Electromagnetic compatibility and radio spectrum matters (ERM) EN300 328-1 (2001-12) EN300 328-2 (2001-12) · Electromagnetic Compatibility (EMC) Standard for radio equipment and services EN301 489-1 EN301 489-17 · Safety Test EN60950 Intended for use in the following countries: Austria Belgium Denmark Finland France Germany Italy Luxembourg Netherlands Norway Spain Sweden Switzerland United Kingdom Portugal Greece Ireland Iceland v COMPLIANCES Safety Compliance Wichtige Sicherheitshinweise (Germany) 1.

Bitte lesen Sie diese Hinweise sorgfältig durch. 2. Heben Sie diese Anleitung für den späteren Gebrauch auf. 3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwe. . . . .

. . . . .
. . . . . .

 Congratulations on your purchase of the ADSL BarricadeTM g, hereafter referred to as the "Barricade". We are proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet. For those who want to surf the Internet in the most secure way, this router provides a convenient and powerful solution. About the Barricade The Barricade provides Internet access to multiple users by sharing a single-user account. Support is provided for both wired and wireless devices. New technology provides wireless security via Wired Equivalent Privacy (WEP) encryption and MAC address filtering. It is simple to configure and can be up and running in minutes.

Features and Benefits · · · · Internet connection to an ADSL modem via an RJ-11 ADSL port Local network connection via four 10/100 Mbps Ethernet ports On-board IEEE 802.11g wireless network adapter DHCP for dynamic IP configuration, and DNS for domain name mapping 1-1 INTRODUCTION · · Firewall with Stateful Packet Inspection, client privileges, intrusion detection, and NAT NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet services such as web, FTP, e-mail, and Telnet) VPN pass-through (IPSec-ESP Tunnel mode, L2TP, PPTP) User-definable application sensing tunnel supports applications requiring multiple connections Easy setup through a web browser on any operating system that supports TCP/IP Compatible with all popular Internet applications · · · · Applications Many advanced networking features are provided by the Barricade: · Wireless and Wired LAN The Barricade provides connectivity to 10/100 Mbps devices, and wireless IEEE 802.11g compatible devices, making it easy to create a network in small offices or homes. · Internet Access This device supports Internet access through an ADSL connection. Since many DSL providers use PPPoE or PPPoA to establish communications with end users, the Barricade includes built-in clients for these protocols, eliminating the need to install these services on your computer. 1-2 APPLICATIONS · Shared IP Address The Barricade provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can browse the web at the same time. · Virtual Server If you have a fixed IP address, you can set the Barricade to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the Barricade can route the request to the appropriate server (at another internal IP address).
This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network. · DMZ Host Support Allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly. · Security The Barricade supports security features that deny Internet access to specified users, or filter all requests for specific services that the administrator does not want to serve. The Barricade's firewall also blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.
WEP (Wired Equivalent Privacy), SSID, and MAC filtering provide security over the wireless network. 1-3 INTRODUCTION · Virtual Private Network (VPN) The Barricade supports three of the most commonly used VPN protocols -- PPTP, L2TP, and IPSec. These protocols allow remote users to establish a secure connection to their corporate network. If your service provider supports VPNs, then these protocols can be used to create an authenticated and encrypted tunnel for passing secure data over the Internet (i.e.
, a traditionally shared data network). The VPN protocols supported by the Barricade are briefly described below. · Point-to-Point Tunneling Protocol --

Provides a secure tunnel for remote client access to a PPTP security gateway. PPTP includes provisions for call origination and flow control required by ISPs. L2TP merges the best features of PPTP and L2F -- Like PPTP, L2TP requires that the ISP's routers support the protocol. IP Security -- Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication. · · 1-4 CHAPTER 2 INSTALLATION Before installing the ADSL BarricadeTM g, verify that you have all the items listed under the Package Contents list. If any of the items are missing or damaged, contact your local distributor. Also be sure that you have all the necessary cabling before installing the Barricade.

After installing the Barricade, refer to "Configuring the Barricade" on page 4-1. Package Contents After unpacking the Barricade, check the contents of the box to be sure you have received the following components: · · · · · · Barricade ADSL Router (SMC7804WBRB) Power adapter One CAT-5 Ethernet cable (RJ-45) Telephone patch cable (RJ-11) Quick install guide Documentation CD Immediately inform your dealer in the event of any incorrect, missing, or damaged parts.

If possible, please retain the carton and original packing materials in case there is a need to return the product. 2-1 INSTALLATION System Requirements You must meet the following minimum requirements: · · ADSL line installed by your Internet Service Provider. A PC using a fixed IP address or dynamic IP address assigned via DHCP, as well as a gateway server address and DNS server address from your service provider. A computer equipped with a 10/100 Mbps network adapter, a USB-to-Ethernet converter or an IEEE 802.11g wireless network adapter. TCP/IP network protocols installed on each PC that will access the Internet. A Java-enabled web browser, such as Microsoft Internet Explorer 5.0 or above installed on one PC at your site for configuring the Barricade.

· · · Hardware Description The Barricade contains an integrated ADSL modem and connects to the Internet or to a remote site using its RJ-11 WAN port. It can be connected directly to your PC or to a local area network using any of the four Fast Ethernet LAN ports. Access speed to the Internet depends on your service type. Full-rate ADSL provides up to 8 Mbps downstream and 640 kbps upstream. G.

lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 kbps upstream. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits. Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet ports and 54 Mbps over the built-in wireless network adapter. 2-2 HARDWARE DESCRIPTION The Barricade includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting.

It also provides the following ports on the rear panel: 4 3 2 1 LAN Reset DC12V 1.25A Max. ADSL/RJ11 LAN Ports Reset Button Power Inlet WAN Port Figure 2-1. Rear Panel Item LAN Ports Reset Button Description Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch). Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see "Reset" on page 4-62. Connect the included power adapter to this inlet.

Warning: Using the wrong type of power adapter may damage the Barricade. ADSL Port WAN port (RJ-11). Connect your ADSL line to this port. Power Inlet 2-3 INSTALLATION LED Indicators The power and port LED indicators on the front panel are illustrated by the following figure and table. ADSL BARRICADE Figure 2-2. Front Panel LED PWR Status On Off ADSL SYN On Flashing Off ADSL DATA Flashing Off WLAN LAN (4 LEDs) Flashing On Flashing Off Description The Barricade is receiving power. Normal operation. Power off or failure. ADSL connection is functioning correctly. The Barricade is establishing an ADSL link.

ADSL connection is not established. The indicated ADSL port is sending or receiving data. No data is being transferred. The WLAN port is sending or receiving data. Ethernet connection is established.

The indicated LAN port is sending or receiving data. There is no LAN connection on the port. 2-4 ISP SETTINGS ISP Settings Please collect the following information from your ISP before setting up the Barricade: · · · · ISP account user name and password Protocol, encapsulation and VPI/VCI circuit numbers DNS server address IP address, subnet mask and default gateway (for fixed IP users only) Connect the System The Barricade can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines: · · Keep the Barricade away from any heating devices.

Do not place the Barricade in a dusty or wet environment. You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the Barricade. Connect the ADSL Line Connect the supplied RJ-11 cable from the ADSL Microfilter/Splitter to the ADSL port on your Barricade. When inserting an ADSL RJ-11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. 2-5 INSTALLATION Phone Line Configuration Installing a Full-Rate Connection If you are using a full-rate (G.dmt) connection, your service provider will attach the outside ADSL line to a data/voice splitter. In this case you can connect your phones and computer directly to the splitter as shown below: Plain Old Telephone System (POTS) Voice Residential Connection Point [Network Interface Device (NID)] Voice & Data Filter Voice & Data Data ADSL Router or Ethernet hub or switch Figure 2-3. Installing with a Splitter 2-6 CONNECT THE SYSTEM Installing a Splitterless Connection If you are using a splitterless (G.lite) connection, then your service provider will attach the outside ADSL line directly to your phone system. In this case you can connect your phones and computer directly to the incoming ADSL line, but you will have to add low-pass filters to your phones as shown below: Plain Old Telephone System (POTS) Voice Residential Connection Point [Network Interface Device (NID)] Voice & Data Filter Voice & Data Data ADSL Router or Ethernet hub or switch Figure 2-4.

Installing without a Splitter 2-7 INSTALLATION Attach to Your Network Using Ethernet Cabling The four LAN ports on the Barricade auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half duplex or full duplex. Use RJ-45 cables to connect any of the four LAN ports on the Barricade to an Ethernet adapter on your PC. Otherwise, cascade any of the LAN ports on the Barricade to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that it is properly seated. Warning: Do not plug a phone jack connector into an RJ-45 port. This may damage the Barricade. Notes: 1. Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. Use Category 3, 4, or 5 for connections that operate at 10 Mbps, and Category 5 for connections that operate at 100 Mbps. 2.

Make sure each twisted-pair cable length does not exceed 100 meters (328 feet). Connect the Power Adapter Plug the power adapter into the power socket on the rear of the Barricade, and the other end into a power outlet. Check the power indicator on the front panel is lit. If the power indicator is not lit, refer to "Troubleshooting" on page A-1. In case of a power input failure, the Barricade will automatically restart and begin to operate once the input power is restored.

2-8 CHAPTER 3 CONFIGURING CLIENT PC After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the Barricade.

See: "Windows 98/Me" on page 3-2 "Windows NT 4.0" on page 3-7 "Windows 2000" on page 3-11 "Windows XP" on page 3-14 or "Configuring Your Macintosh Computer" on page 3-16 depending on your operating system. 3-1 CONFIGURING CLIENT PC TCP/IP Configuration To access the Internet through the Barricade, you must configure the network settings of the computers on your LAN to use the same IP subnet as the Barricade. The default IP settings for the Barricade are: IP Address: 192.

168.2.1 Subnet Mask: 255.255.255.0 Note: These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the Barricade's web configuration interface in order to make the required changes. (See "Configuring the Barricade" on page 4-1 for instruction on configuring the Barricade.) Windows 98/Me You may find that the instructions in this section do not exactly match your version of Windows. This is because these steps and screen shots were created from Windows 98. Windows Millennium Edition is similar, but not identical, to Windows 98.

1. On the Windows desktop, click Start/Settings/Control Panel. 3-2 WINDOWS 98/ME 2. In Control Panel, double-click the Network icon. 3. In the Network window, under the Configuration tab, double-click the TCP/IP item listed for your network card. 4. In the TCP/IP window, select the IP Address tab. If "Obtain an IP address automatically" is already selected, your computer is already configured for DHCP. If not, select this option.

3-3 CONFIGURING CLIENT PC 5. Windows may need your Windows 95/98/Me CD to copy some files. After it finishes copying, it will prompt you to restart your system. Click Yes and your computer will restart. TCP/IP Configuration Setting Primary DNS Server Secondary DNS Server Default Gateway Host Name ____.

____.____.____ ____.____.____.

____ ____.____.____.____ ____.____.____.____ Disable HTTP Proxy You need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. The following steps are for Internet Explorer. Internet Explorer 1.

Open Internet Explorer. 2. Click the Stop button, then click Tools/Internet Options. 3-4 WINDOWS 98/ME 3. In the Internet Options window, click the Connections tab. Next, click the LAN Settings... button. 4.

Clear all the check boxes. 5. Click OK, and then click OK again to close the Internet Options window. 3-5 CONFIGURING CLIENT PC Obtain IP Settings from Your ADSL Router Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can also verify that you have configured your computer correctly.

1. On the Windows desktop, click Start/Run... 2.

Type "WINIPCFG" and click OK. It may take a second or two for the IP Configuration window to appear. 3. In the IP Configuration window, select your network card from the drop-down menu. Click Release and then click Renew. Verify that your IP address is now 192.168.2.xxx, your Subnet Mask is 255.255.

255.0 and your Default Gateway is 192.168.2.1. These values confirm that your Barricade is functioning. Click OK to close the IP Configuration window. 3-6 WINDOWS NT 4.0 Windows NT 4.0 1.

On the Windows desktop, click Start/Settings/Control Panel. 2. Double-click the Network icon. 3-7 CONFIGURING CLIENT PC 3. In the Network window, Select the Protocols tab.

Double-click TCP/IP Protocol. 4. When the Microsoft TCP/IP Properties window open, select the IP Address tab. 5. In the Adapter drop-down list, be sure your Ethernet adapter is selected.

6. If "Obtain an IP address automatically" is already selected, your computer is already configured for DHCP. If not, select this option and click "Apply." 7. Click the DNS tab to see the primary and secondary DNS servers. Record these values, and then click "Remove." Click "Apply", and then "OK." 3-8 WINDOWS NT 4.0 8. Windows may copy some files, and will then prompt you to restart your system.

Click Yes and your computer will shut down and restart. TCP/IP Configuration Setting Default Gateway Primary DNS Server Secondary DNS Server Host Name ____.____.____.____ ____.____.____.____ ____.____.____.____.

____ ____.____.____.____ Disable HTTP Proxy You need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages.

Determine which browser you use and refer to "Internet Explorer" on page 3-4. Obtain IP Settings from Your Barricade Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you will verify that you have configured your computer correctly. 1. On the Windows desktop, click Start/Programs/ Command Prompt.

3-9 CONFIGURING CLIENT PC 2. In the Command Prompt window, type "IPCONFIG /RELEASE" and press the ENTER key. 3. Type "IPCONFIG /RENEW" and press the ENTER key. Verify that your IP Address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.

0 and your Default Gateway is 192.168.2.1 These values confirm that your Barricade is functioning. 4. Type "EXIT" and press the ENTER key to close the Command Prompt window. Your computer is now configured to connect to the Barricade. 3-10 WINDOWS 2000 Windows 2000 1. On the Windows desktop, click Start/Settings/Network and Dial-Up Connections. 2.

Click the icon that corresponds to the connection to your Barricade. 3. The connection status screen will open. Click Properties. 4.

Double-click Internet Protocol (TCP/IP). 5. If "Obtain an IP address automatically" and "Obtain DNS server address automatically" are already selected, your computer is already configured for DHCP. If not, select this option. 3-11 CONFIGURING CLIENT PC Disable HTTP Proxy You need to verify that the "HTTP Proxy" feature of your web browser is disabled.

This is so that your browser can view the Barricade's HTML configuration pages. Determine which browser you use and refer to "Internet Explorer" on page 3-4. Obtain IP Settings from Your Barricade Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly. 1. On the Windows desktop, click Start/Programs/ Accessories/Command Prompt. 2. In the Command Prompt window, type "IPCONFIG/RELEASE" and press the ENTER key. 3-12 WINDOWS 2000 3. Type "IPCONFIG /RENEW" and press the ENTER key.

Verify that your IP Address is now 192.168.

2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168.2.1 These values confirm that your ADSL Router is functioning. 4. Type "EXIT" and press the ENTER key to close the Command Prompt window. Your computer is now configured to connect to the Barricade. 3-13 CONFIGURING CLIENT PC Windows XP 1. On the Windows desktop, click Start/Control Panel. 2. In the Control Panel window, click Network and Internet Connections. 3. The Network Connections window will open. Double-click the connection for this device. 4. On the connection status screen, click Properties. 5. Double-click Internet Protocol (TCP/IP). 6. If "Obtain an IP address automatically" and "Obtain DNS server address automatically" are already selected, your computer is already configured for DHCP. If not, select this option. Disable HTTP Proxy You need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. Determine which browser you use and refer to "Internet Explorer" on page 3-4.

Obtain IP Settings from Your Barricade Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly. 1. On the Windows desktop, click Start/Programs/Accessories/ Command Prompt. 3-14 WINDOWS XP 2. In the Command Prompt window, type "IPCONFIG/RELEASE" and press the ENTER key. 3. Type "IPCONFIG /RENEW" and press the ENTER key. Verify that your IP Address is now 192.168. 2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192. 168.2.1. These values confirm that your ADSL router is functioning. Type "EXIT" and press the ENTER key to close the Command Prompt window. Your computer is now configured to connect to the Barricade. 3-15 CONFIGURING CLIENT PC Configuring Your Macintosh Computer You may find that the instructions here do not exactly match your operating system. This is because these steps and screenshots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2. Follow these instructions: 1. Pull down the Apple Menu System Preferences . Click 2.

Double-click the Network icon in the Systems Preferences window. 3-16 CONFIGURING YOUR MACINTOSH COMPUTER 3. If "Using DHCP Server" is already selected in the Configure field, your computer is already configured for DHCP. If not, select this Option. 4. Your new settings are shown on the TCP/IP tab. Verify that your IP Address is now 192.168.2.xxx, your Subnet Mask is 255. 255.255.0 and your Default Gateway is 192.168.2. 1. These values confirm that your Barricade is functioning. 5. Close the Network window. Now your computer is configured to connect to the Barricade. Disable HTTP Proxy You need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. The following steps are for Internet Explorer. Internet Explorer 1. Open Internet Explorer and click the Stop button. Click Explorer/Preferences. 2. In the Internet Explorer Preferences window, under Network, select Proxies. 3-17 CONFIGURING CLIENT PC 3. Uncheck all check boxes and click OK.

3-18 CHAPTER 4 CONFIGURING THE BARRICADE After you have configured TCP/IP on a client computer, you can configure the Barricade using Internet Explorer 5.0 or above. To access the Barricade's management interface, enter the default IP address of the Barricade in your web browser: http://192.168.2.1. Enter the default password: "smcadmin", and click "LOGIN". 4-1 CONFIGURING THE BARRICADE Navigating the Management Interface The Barricade's management interface consists of a Setup Wizard and an Advanced Setup section. Setup Wizard: Use the Setup Wizard if you want to quickly set up the Barricade. Go to "Setup Wizard" on page 4-3. Advanced Setup: Advanced Setup supports more advanced functions like hacker attack detection, IP and MAC address filtering, virtual server setup, virtual DMZ host, as well as other functions. Go to "Advanced Setup" on page 4-13. Making Configuration Changes Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, click the "APPLY" or "NEXT" button at the bottom of the page to enable the new setting. Note: To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5. 0 is configured as follows: Under the menu Tools/Internet Options/General/Temporary Internet Files/Settings, the setting for "Check for newer versions of stored pages" should be "Every visit to the page." 4-2 SETUP WIZARD Setup Wizard Time Zone Click on "Setup Wizard". The first item in the Setup Wizard is Time Zone. For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop-down list. If your area requires it, check to enable the clock for daylight saving changes, and enter the Daylight Savings Time start and end dates for your location. If you want to automatically synchronize the ADSL router with a public time server, check the box to enable Enable Automatic Time Server Maintenance. Select the desired servers from the drop down menu. Click "NEXT" to continue. Note: Units sold in the United States are configured by default to use only radio channels 1-11 as defined by FCC regulations. Units sold in other countries are configured by default without a country code (i.e., 99). Setting the country code restricts operation of the device to the radio channels permitted for the wireless networks in the specified country. 4-3 CONFIGURING THE BARRICADE Parameter Setting Select your Country and Internet Service Provider.

This will automatically configure the Barricade with the correct Protocol, Encapsulation and VPI/VCI settings for your ISP. If your Country or Internet Service Provider is not listed you will need to manually enter settings. Go to "Parameter Setting - Country or ISP Not Listed" on page 4-7 in the manual. If your ISP uses Protocols PPPoA or PPPoE you will need to enter the username, password and DNS Server address supplied by your ISP. If your ISP uses Protocol RFC1483 Routed you will need to enter the IP address, Subnet Mask, Default Gateway and DNS Server address supplied by your ISP. Note: By default 192.168.2.1 is set for the DNS Server address, this needs to be changed to reflect your ISP's DNS Server address. Click "NEXT" to continue. 4-4 SETUP WIZARD Confirm The Confirm page shows a summary of the configuration parameters. Check ADSL operation mode (WAN), Network Layer Parameters (WAN) and ISP parameters are correct.

Parameter ADSL Operation Mode (WAN) ISP Protocol VPI/VCI Description The type of ISP you have selected. Indicates the protocol used. Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI).

AAL5 Encapsulation Shows the packet encapsulation type. Go to page 4-20 for a detailed description. Network Layer Parameters (WAN) IP Address Subnet Mask Default Gateway DNS Server ISP Parameters Username Password The ISP assigned user name. The password (hidden). WAN IP address (only displayed if you have static IP).

WAN subnet mask (only displayed if you have static IP). WAN gateway (only displayed if you have static IP). The IP address of the DNS server. 4-5 CONFIGURING THE BARRICADE Parameter DHCP Parameters Function Default Gateway Subnet Mask Name Server 1 Name Server 2 Start IP Address Number of IP Shows the DHCP function is enabled or disabled. LAN IP address of the Barricade. The network subnet mask. Primary DNS server IP address. Alternate DNS server IP address. Start IP address of DHCP assigned IP addresses. Number of IP addresses available for assignment by the DHCP server.

Description If the parameters are correct, click "APPLY" to save these settings. Your Barricade is now set up. Go to "Troubleshooting" on page A-1 if you cannot make a connection to the Internet. 4-6 SETUP WIZARD Parameter Setting - Country or ISP Not Listed If your Country or Internet Service Provider is not listed select "Others". @@@@@@@@@@@@@@@@@@@@@@@@@@@@@Select the encapsulation used by ISP from the drop down list. Enter the ISP assigned user name. Enter your password. @@@@@@Select the encapsulation used by ISP from the drop down list. Enter the ISP assigned user name. Enter your password.

@@@@Enter the subnet mask address provided by your ISP. Enter the gateway address provided by your ISP. Enter the Domain Name Server address. @@@@@@@@Specifies the Internet connection settings. Sets the TCP/IP configuration for the Barricade LAN interface and DHCP clients. Configures the radio frequency, SSID, and security for wireless communications. Configures Address Mapping, virtual server and special applications. Sets the routing parameters and displays the current routing table. Configures a variety of security and specialized functions including: Access Control, URL blocking, Internet access control scheduling, intruder detection, and DMZ. Community string and trap server settings.

Sets the ADSL operation type and shows the ADSL status. WAN LAN Wireless NAT Routing Firewall SNMP ADSL 4-13 CONFIGURING THE BARRICADE Menu DDNS UPnP Tools Description Dynamic DNS provides users on the Internet with a method to tie their domain name(s) to a Dynamic or Static IP address. Allows you to enable or disable the Universal Plug and Play function. Contains options to backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system. Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and firewall information. Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number. Shows the security and DHCP client log. Status 4-14 ADVANCED SETUP System Time Settings Select your local time zone from the drop down list. This information is used for log entries and client filtering. For accurate timing of log entries and system events, you need to set the time zone.

Select your time zone from the drop down list. If you want to automatically synchronize the ADSL router with a public time server, check the box to Enable Automatic Time Server Maintenance. Select the desired servers from the drop down menu. 4-15 CONFIGURING THE BARRICADE Password Settings Use this page to change the password for accessing the management interface of the Barricade. Passwords can contain from 3~12 alphanumeric characters and are case sensitive. Note: If you lost the password, or you cannot gain access to the user interface, press the blue reset button on the rear panel, holding it down for at least five seconds to restore the factory defaults. The default password is "smcadmin". Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity. If the connection is inactive for longer than the maximum idle time, it will perform system logout, and you have to log in again to access the management interface. (Default: 10 minutes) 4-16 ADVANCED SETUP Remote Management By default, management access is only available to users on your local network.

However, you can also manage the Barricade from a remote host by entering the IP address of a remote computer on this screen. Check the Enabled check box, and enter the IP address of the Host Address and click "APPLY". Note: If you check Enable and specify an IP address of 0.0.0.

0, any remote host can manage the Barricade. For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by :8080, for example, 212.120.68.

20:8080. 4-17 CONFIGURING THE BARRICADE DNS Domain Name Servers (DNS) are used to map a domain name (e.g., www.smc.com) with the IP address (e.g., 64.147.25.

20). Your ISP should provide the IP address of one or more Domain Name Servers. Enter those addresses on this page, and click "APPLY". 4-18 ADVANCED SETUP WAN Specify the WAN connection parameters provided by your Internet Service Provider (ISP). The Barricade can be connected to your ISP in one of the following ways: PPPoE ATM Clone MAC ISP 4-19 CONFIGURING THE BARRICADE PPPoE Enter the PPPoE (Point-to-Point over Ethernet) parameters here. Parameter Enable/Disable IP Address Description Enables/disables the PPPoE function. If your IP address is assigned by the ISP each time you connect, leave this field all zeros. Otherwise, enter your ISP supplied static IP address here. If your subnet mask is assigned by the ISP each time you connect, leave this field all zeros. Otherwise, enter your subnet mask here.

Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). Specifies how to handle multiple protocols at the ATM transport layer. · VC-MUX: Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead. LLC: Point-to-Point Protocol over ATM Logical Link Control (LLC) allows multiple protocols running over one virtual circuit (using slightly more overhead). Subnet Mask VPI/VCI Encapsulation · Dial on demand Check this box to automatically connect to your ISP.

4-20 ADVANCED SETUP Parameter Idle Time (Minute) Description Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. Choose the ISP to whom this connection will apply.

ISP Name ATM Enter ATM (Asynchronous Transfer Mode) function parameters here. Parameter Protocol Description · · Disable: Disables the ATM mode. 1483 Bridging: Bridging is a standardized layer 2 technology. It is typically used in corporate networks to extend the physical reach of a single LAN segment and increase the number of stations on a LAN without compromising performance. Bridged data is encapsulated using the RFC1483 protocol to enable data transport. IP Address Subnet Mask VPI/VCI IP address of the ATM interface. Subnet mask of the ATM interface. Each connection must have a unique pair of VPI/VCI settings. Default Gateway Default gateway of the ATM interface. 4-21 CONFIGURING THE BARRICADE Parameter Encapsulation Description Specifies how to handle multiple protocols at the ATM transport layer. Go to"Encapsulation" on page 4-20, for a detailed description. Check this box if your ISP assigns an IP to clients using DHCP.

DHCP Client Clone MAC Address Some ISPs require you to register your MAC address with them. If this is the case, the MAC address of the Barricade must be changed to the MAC address that you have registered with your ISP. 4-22 ADVANCED SETUP ISP Enter the Internet Service Provider (ISP) name, user name, and password for each ISP connection you have. You can enter up to four sets of information here. 4-23 CONFIGURING THE BARRICADE LAN Use the LAN menu to configure the LAN IP address and to enable the DHCP server for dynamic client address allocation. Parameter LAN IP IP Address DHCP Server Lease Time Description The IP address of the Barricade. The Barricade comes with the DHCP function. To dynamically assign an IP address to client PCs, enable this function. Set the IP lease time. For home networks this may be set to Forever, which means there is no time limit on the IP address lease. IP Subnet Mask The subnet mask of the network. IP Address Pool Start IP Address Specify the start IP address of the DHCP pool. Do not include the gateway address of the Barricade in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e. , 192.168.2.xxx. End IP Address Specify the end IP address of the DHCP pool.
Domain Name If your network uses a domain name, enter it here. Otherwise, leave this field blank. Note: Remember to configure your client PCs for dynamic address allocation. (See page 3-2 for details.) 4-24 ADVANCED SETUP Wireless The Barricade also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, all you need to do is enable the wireless function, define the radio channel, the domain identifier, and the security options. Check Enable and click "APPLY". 4-25 CONFIGURING THE BARRICADE Channel and SSID You must specify a common radio channel and SSID (Service Set ID) to be used by the Barricade Wireless Router and all of its wireless clients. Be sure you configure all of its clients to the same values. Parameter ESSID ESSID Broadcast Wireless Mode Description Extended Service Set ID.

The ESSID must be the same on the Barricade and all of its wireless clients. Enable or disable the broadcasting of the SSID. This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have. Transmission Rate The default is Fully Automatic. The transmission rate is automatically adjusted based on the receiving data error rate. Usually the connection quality will vary depending on the distance between the wireless router and wireless adapter. You can also select a lower transmission data rate to maximize the radio communication range. Channel The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the Barricade and all of its wireless clients.
The Barricade will automatically assign itself a radio channel, or you may select one manually. g Nitro This is the turbo function for the 11g wireless network. Make sure your clients also support this function before you enable it. 4-26 ADVANCED SETUP Security To make your wireless network safe, you should turn on the security function. The Barricade supports WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected) security mechanisms.
4-27 CONFIGURING THE BARRICADE WEP If you want to use WEP to protect your wireless network, you need to set the same parameters for the Barricade and all your wireless clients. Parameter WEP Mode Key Provisioning Description Select 64 bit or 128 bit key to use for encryption. Select Static if there is only one fixed key for encryption. If you want to select Dynamic, you would need to enable 802.1X function first.
You may automatically generate encryption keys or manually enter the keys. To generate the key automatically with passphrase, check the Passphrase box, enter a string of characters. Select the default key from the drop down menu. Click "APPLY". Note: The passphrase can consist of up to 32 alphanumeric characters. To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F.) Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet. 4-28 ADVANCED SETUP WPA Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1X mechanisms.

It provides dynamic key encryption and 802.1X authentication service. Parameter Cypher suite Authentication Description The security mechanism used in WPA for encryption. Choose 802.1X or Pre-shared Key to use as the authentication method. ·802.1X: for the enterprise network with a RADIUS server. ·Pre-shared key: for the SOHO network environment without an authentication server. Pre-shared key type Select the key type to be used in the Pre-shared Key. Pre-shared Key Group Key ReKeying Type in the key here.
The period of renewing broadcast/multicast key. 4-29 CONFIGURING THE BARRICADE 802.1X If 802.1X is used in your network, then you should enable this function for the Barricade. Parameter 802.
1X Authentication Session Idle timeout Description Enable or disable this authentication function. Defines a maximum period of time for which the connection is maintained during inactivity. Re-Authentication Defines a maximum period of time for which the Period authentication server will dynamically re-assign a session key to a connected client. Quiet Period Server Type RADIUS Server Parameters Server IP Server Port Secret Key NAS-ID The IP address of your authentication server. The port used for the authentication service.
The secret key shared between the authentication server and its clients. Defines the request identifier of the Network Access Server.

Defines a maximum period of time for which the Barricade will wait between failed authentications. Select TINY or RADIUS as the authentication server. 4-30 ADVANCED SETUP NAT Network Address Translation allows multiple users to access the Internet sharing one public IP. 4-31 CONFIGURING THE BARRICADE Address Mapping Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP into the "from" field. 4-32 ADVANCED SETUP Virtual Server If you configure the Barricade as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses.

In other words, depending on the requested service (TCP/UDP port number), the Barricade redirects the external service request to the appropriate server (located at another internal IP address). For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them. The more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

A list of ports is maintained at the following link: http://www.iana.org/assignments/port-numbers. Note: The WAN interface should have a fixed IP address to best utilize this function. See "DDNS" on page 4-58 for using the same domain name even though your IP address changes each time you log into the ISP. 4-33 CONFIGURING THE BARRICADE Special Application Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony. These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these pages to specify the additional public ports to be opened for each application. 4-34 ADVANCED SETUP Routing These pages define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters. 4-35 CONFIGURING THE BARRICADE Static Route Parameter Index Network Address Subnet Mask Gateway Description Check the box of the route you wish to delete or modify.

Enter the IP address of the remote computer for which to set a static route. Enter the subnet mask of the remote network for which to set a static route. Enter the WAN IP address of the gateway to the remote network. Click "Add" to add a new static route to the list, or check the box of an already entered route and click "Modify". Clicking "Delete" will remove an entry from the list. 4-36 ADVANCED SETUP RIP Parameter General RIP Parameters RIP mode Auto summary Description Globally enables or disables RIP. If Auto summary is disabled, then RIP packets will include sub-network information from all subnetworks connected to the router. If enabled, this sub-network information will be summarized to one piece of information covering all subnetworks. Table of current Interface RIP parameter Interface Operation Mode The WAN interface to be configured. Disable: RIP disabled on this interface.

Enable: RIP enabled on this interface. Silent: Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts. Version Poison Reverse Sets the RIP (Routing Information Protocol) version to use on this interface. A method for preventing loops that would cause endless retransmission of data traffic. 4-37 CONFIGURING THE BARRICADE Parameter Authentication Required Description · · None: No authentication. Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets. MD5: An algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual.

· Authentication Code Password or MD5 Authentication key. RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. RIP routers maintain only the best route to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.

4-38 ADVANCED SETUP Routing Table Parameter Flags Description Indicates the route status: C = Direct connection on the same subnet. S = Static route. R = RIP (Routing Information Protocol) assigned route. I = ICMP (Internet Control Message Protocol) Redirect route. Network Address Netmask Destination IP address.

The subnetwork associated with the destination. This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a "1" is part of the subnet mask number; each bit that corresponds to "0" is part of the host number. Gateway Interface Metric The IP address of the router at the next hop to which frames are forwarded. The local interface through which the next hop of this route is reached. When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. 4-39 CONFIGURING THE BARRICADE Firewall The Barricade Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks. Network attacks that deny access to a network device are called Denial-ofService (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (See page 4-46 for details.) The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network.