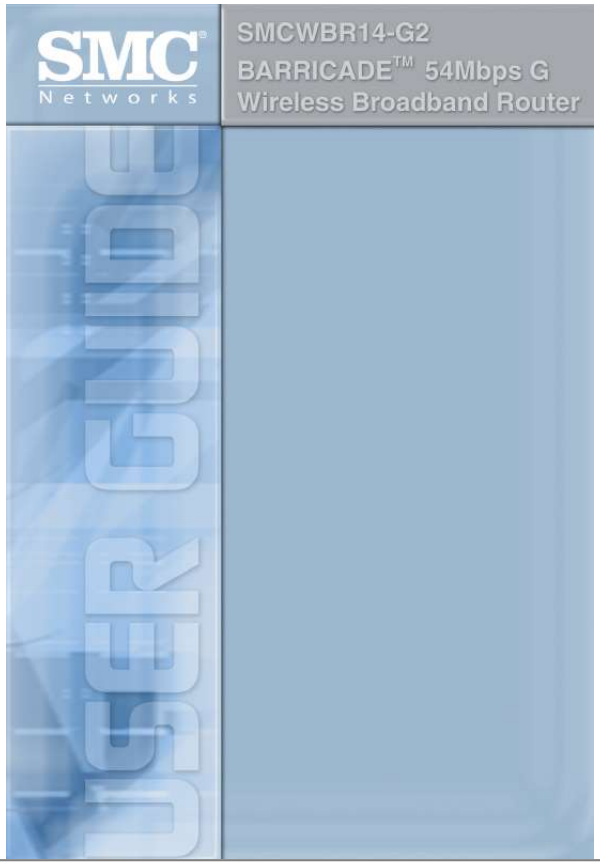

Manual abstract:

38 Tesla Irvine, CA 92618 All rights reserved. Trademarks: 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 Warranty terms may differ according to geographic region. For complete details please consult your country's support section of the SMC web site, http://www.smc.com 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 the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the distance 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: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. · · · IMPORTANT NOTE: 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 between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. IEEE 802.11b or 802.11g operation of this product in the U.S.

A. is firmware-limited to channels 1 through 11. iii COMPLIANCES Industry Canada Statement Operation is subject to the following two conditions: 1. this device may not cause interference and 2. this device must accept any interference, including interference that may cause undesired operation of the device To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing. This device has been designed to operate with an antenna having a maximum gain of 1.5 dBi. Any antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication. To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing. EC Declaration of Conformity SMC contact for these products in Europe is: SMC Networks Europe, Edificio Conata II, Calle Fructuos Gelabert 6-8, 2o, 4a, 08970 - Sant Joan Despi, Barcelona, Spain. Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards: EN 300 328-1 December 2001 V1.3.1 EN 300 328-2 December 2001 V1.2.1 EN 301 489-1 September 2001 V1.

4.1 EN 301 489-17 September 2000 V1.2.1 EN 60950 January 2000 iv COMPLIANCES Countries of Operation & Conditions of Use in the European Community This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below: Note: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below. · This device requires that the user or installer properly enter the current country of operation in the command line interface as described in the user guide, before operating this device. This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other system. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document.

This device may be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1 - 13. · · Declaration of Conformity in Languages of the European Community English Hereby, SMC Networks, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. Valmistaja SMC Networks vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. Hierbij verklaart SMC Networks dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze SMC Networks dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC. French Par la présente SMC Networks déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE Finnish Dutch v COMPLIANCES Swedish Härmed intygar SMC Networks att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG. Undertegnede SMC Networks erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF Hiermit erklärt SMC Networks, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt SMC Networks die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien) Greek Danish German Italian Con la presente SMC Networks dichiara che questo Radio LANach der EN 60950 geprüft ist. Ausgangswerte der Stromversorgung sollten die Werte von AC 7,5-8 V, 50-60 Hz nicht über oder unterschreiten sowie den minimalen Strom von 1 A nicht unterschreiten.

Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70 dB(A) oder weniger. 1. 2. 3. viii TABLE OF CONTENTS 1 Introduction . . . . . .

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. WPA/WPA2, WEP, SSID, and MAC filtering provide security over the wireless network. · Virtual Private Network (VPN Pass-through) The Barricade supports three of the most commonly used VPN protocols PPTP, L2TP, and IPSec.

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 Barricade, verify that you have all the items listed under "Package Contents." 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 54Mbps g Wireless Broadband Router (SMCWBR14-G2) Power adapter One CAT-5 Ethernet cable (RJ-45) One documentation CD Quick Install Guide 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: · · · · Internet access from your local telephone company or Internet Service Provider (ISP) using a DSL modem or cable modem. A computer with a CD-ROM drive Windows (98 or later), MacOS (9.x) An up to date web browser: · · Internet Explorer 5.5 or later Mozilla 1.7/Firefox 1.0 or later Hardware Description The Barricade connects to the Internet or to a remote site using its WAN RJ-45 port linked to a modem. It also can be connected directly to your PC or to a local area network using the Fast Ethernet LAN port. Access speed to the Internet depends on your service type.

Full-rate ADSL provides up to 8 Mbps downstream and 1 Mbps 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 port and 54 Mbps over the built-in wireless network adapter. The Barricade includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting. 2-2 HARDWARE DESCRIPTION Figure 2-1. Front LED indicators The power and port LED indicators on the front panel are illustrated by the following table. LED Power Status On Off WAN On Off PPPoE/DSL On Flashing Off WLAN On Flashing Off Description The Barricade is receiving power.

Normal operation. Power off or failure. WAN link. No WAN link. PPPoE/DSL connection is functioning correctly. The Barricade is sending or receiving data via PPPoE/DSL link. PPPoE/DSL connection is not established. WLAN link. The Barricade is sending or receiving data via WLAN. No WLAN link.

2-3 INSTALLATION LED LAN 1~4 Status On Flashing Off Description Ethernet link. The LAN port is sending or receiving data. No Ethernet link. The following figure and table shows the rear panel of the Barricade. 9V 1A WAN LAN4 LAN3 LAN2 LAN1 Power Connector RJ-45 Port RJ-45 LAN Ports Reset Button Antenna Figure 2-2. Rear Panel Item Power Inlet Description Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may cause damage. WAN Port LAN Ports WAN port (RJ-45). Connect your WAN line to this port. Fast Ethernet ports (RJ-45).

Connect devices on your local area network to these ports (i.e., a PC, hub, switch or IP set top box). Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see "Reset" on page 4-60.

Fixed antenna is connected here. Reset Button Antenna 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 Desktop Installation The Barricade can be positioned on any convenient flat surface 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. 2-5 INSTALLATION Wall-Mount Installation There are two wall-mount holes at the bottom of the Barricade. Before drilling two holes into the wall, make sure the holes are 112 mm apart. 112 mm 1. Choose a suitable location for the Barricade. Note: It should be accessible for installing, cabling and maintaining the device. 2. Measure the distance of the two wall-mount holes. 3. Drill two holes into the wall.

4. Insert a screw into each hole. Note: Leave 5 mm exposed of the screw head. 5. Attach the Barricade to the wall with two wall-mount slots, and then slide the device down until the screws fit firmly into the slots of the device. 2-6 CONNECT THE SYSTEM Connecting the Barricade to your LAN 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. Instead, use only twisted-pair cables with RJ-45 connectors that conform with FCC standards. Notes: 1. Use 100-ohm shielded or unshielded twisted-pair cable with RJ45 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 side panel 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. If the Barricade is properly configured, it will take about 30 seconds to establish a connection with the ADSL service provider after powering up. 2-7 INSTALLATION Application Example The following diagram shows a typical network application. 9V 1A WAN LAN1 LAN2 LAN3 LAN4 Phone ADSL 2-8 CHAPTER 3 CONFIGURING THE CLIENT PC After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the Barricade. You can either configure your computer to automatically obtain IP settings (DHCP) or manually configure IP address settings (Static IP). Depending on your operating system see: "Windows 2000" on page 3-3, "Windows XP" on page 3-9, or "Configuring Your Macintosh Computer" on page 3-15. 3-1 TCP/IP CONFIGURATION 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 network 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 instructions on configuring the Barricade.) 3-2 CONFIGURING THE CLIENT PC Windows 2000 DHCP IP Configuration 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. 3-3 TCP/IP CONFIGURATION 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 these options now and click OK. 3-4 CONFIGURING THE CLIENT PC 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. 3-5 TCP/IP CONFIGURATION 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 correctly. 4. Type "EXIT" and press the Enter key to close the Command Prompt window. 3-6 CONFIGURING THE CLIENT PC Manual IP Configuration 1. Follow steps 1-4 in "DHCP IP Configuration" on page 3-3.

2. Select Use the following IP address. Enter an IP address based on the default network 192.168.2.

x (where x is between 2 and 254), and use 255.255.255.0 for the subnet mask. Use 192.

168.2.1 for the Default gateway field. 3. Select Use the following DNS server addresses. 4. Enter the IP address for the Barricade in the Preferred DNS server field. This automatically relays DNS requests to the DNS server(s) provided by your ISP. Otherwise, add a specific DNS server into the Alternate DNS Server field and click OK to close the dialog boxes. 5.

Record the configured information in the following table. TCP/IP Configuration Setting IP Address Subnet Mask Preferred DNS Server Alternate DNS Server Default Gateway ____.____.____.____ ____.____.____.____ ____.____.____.____.

____ ____.____.____.____ ____.____.

____.____ 3-7 TCP/IP CONFIGURATION 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. 1. To disable the proxy in Internet Explorer, click Tools.

Click Internet Options... and then the Connections tab, shown on the right. In the Local Area Network (LAN) settings section, click LAN Settings... to display the Local Area Network (LAN) Settings pop-up window below. 2. In the Proxy server section, ensure the Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections) check box is not ticked.

3. Click OK. 3-8 CONFIGURING THE CLIENT PC Windows XP DHCP IP Configuration 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. Locate and double-click the Local Area Connection icon for the Ethernet adapter that is connected to the Barricade. 4.

In the connection status screen, click Properties. 3-9 TCP/IP CONFIGURATION 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 these options now and click OK. 3-10 CONFIGURING THE CLIENT PC 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. 3-11 TCP/IP CONFIGURATION 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 correctly. 4. Type "EXIT" and press the Enter key to close the Command Prompt window.

Your computer is now configured to connect to the Barricade. 3-12 CONFIGURING THE CLIENT PC Manual IP Configuration 1. Follow steps 1-5 in "DHCP IP Configuration" on page 3-9.

2. Select Use the following IP Address. 3. Enter an IP address based on the default network 192.168.

2.x (where x is between 2 and 254), and use 255.255.255.0 for the subnet mask.

Use 192.168.2.1 for the Default gateway field. 4. Select Use the following DNS server addresses. 5. Enter the IP address for the Barricade in the Preferred DNS server field. This automatically relays DNS requests to the DNS server(s) provided by your ISP. Otherwise, add a specific DNS server into the Alternate DNS Server field and click OK to close the dialog boxes.

6. Record the configured information in the following table. TCP/IP Configuration Setting IP Address Subnet Mask Preferred DNS Server Alternate DNS Server Default Gateway ____.____.____.____ ____.____.____.____ ____.____.____.____ ____.____.____.____ ____.____.____.____ 3-13 TCP/IP CONFIGURATION 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. 1.

To disable the proxy in Internet Explorer, click Tools. Click Internet Options... and then the Connections tab, shown on the right. In the Local Area Network (LAN) settings section, click LAN Settings... to display the Local Area Network (LAN) Settings pop-up window below. 2.

In the Proxy server section, ensure the Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections) check box is not ticked. 3. Click OK. 3-14 CONFIGURING THE 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 screen shots 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. 3-15 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 in 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. 3-16 CONFIGURING THE 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. 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. Uncheck all check boxes and click OK. 3-17 CONFIGURING YOUR MACINTOSH COMPUTER 3-18 CHAPTER 4 CONFIGURING THE BARRICADE After you have configured TCP/IP on a client computer, use a web browser to configure the Barricade. The Barricade can be configured by any Java-supported browser such as Internet Explorer 5.

5 or above. Using the web management interface, you can configure the Barricade and view statistics to monitor network activity. To access the Barricade's management interface, enter the IP address of the Barricade in your web browser: http://192.168.2.

1 (The Barricade automatically switches to Port 80 for management access.) 4-1 CONFIGURING THE BARRICADE Navigating the Web Browser Interface The Barricade's management interface consists of a Setup Wizard, a Home Network Settings section, a Security section and an Advanced Settings section. Setup Wizard: Use the Setup Wizard for quick and easy configuration of your Internet connection and basic LAN settings. Go to "Setup Wizard" on page 4-5. Home Network Settings: Use the Home Network Settings section to configure your LAN, WAN and wireless settings. Go to "Home Network Settings" on page 4-13. Security: In this section, you can easily configure your wireless security settings. Go to "Security" on page 4-27. Advanced Settings: Advanced Settings supports more advanced functions like NAT, system maintenance and UPnP. Go to "Advanced Settings" on page 4-51.

4-2 NAVIGATING THE WEB BROWSER INTERFACE Making Configuration Changes Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click the Apply or Save Settings 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 5.5 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.

4-3 CONFIGURING THE BARRICADE Login Screen The Login screen automatically appears first. Enter the default password "smcadmin" and then click LOGIN. Note: Your password is case sensitive. 4-4 SETUP WIZARD Setup Wizard Getting Started The Setup Wizard automatically appears by clicking on the Setup Wizard button of the left-hand menu. The first item in the Setup Wizard is Getting Started.

Simply click NEXT to proceed to the following screen and configure your Wireless Settings. 4-5 CONFIGURING THE BARRICADE Wireless Settings Enter your wireless network settings on this page. You must specify a common radio channel and SSID (Service Set ID) to be used by the Barricade and all of its wireless clients. Be sure you configure all of its clients to the same value. For security purposes, you should change the default SSID immediately. Parameter Wireless Network Name (SSID) Broadcast Wireless Network Name Description The Service Set ID (SSID) is the name of your wireless network. The SSID must be the same on the Barricade and all of its wireless clients. (Default: SMC) Enable or disable the broadcasting of the SSID. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network "discovery" feature of some products such as Windows XP. (Default: Enable) This device supports the following modes: 11g only, 11b only, and 11b/g mixed mode. (Default: 11b/g Mixed mode) Wireless Mode 4-6 SETUP WIZARD Parameter Wi-Fi Channel Number Description The radio channel used by the Barricade 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. (Default channel: 6) Extend Range Increases the range of the Barricade.

(Default: Disable) 4-7 CONFIGURING THE BARRICADE Internet Settings Specify the WAN connection type required by your Internet Service Provider. Specify Cable modem, Fixed-IP xDSL, PPPoE xDSL or PPTP. Select your connection type to proceed. Click BACK to go back and change your settings. 4-8 SETUP WIZARD Cable Modem Settings If the ISP requires you to input a Host Name, type it in the Host Name field. The MAC Address field will be filled automatically. Click NEXT to proceed, or BACK to change your settings. 4-9 CONFIGURING THE BARRICADE ADSL Settings - Fixed-IP xDSL Enter the IP address, Subnet Mask, and Gateway IP address provided to you by your ISP in the appropriate fields below. Click NEXT to proceed, or BACK to change your settings. 4-10 SETUP WIZARD ADSL Settings - PPPoE Enter the User Name and Password required by your ISP in the appropriate fields.

If your ISP has provided you with a Service Name enter it in the Service Name field, otherwise, leave it blank. Leave the Maximum Transmission Unit (MTU) at the default value (1454) unless you have a particular reason to change it. Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. Check Keep session to keep the session alive.

Check the Auto-connect check box to automatically re-establish the connection as soon as you attempt to access the Internet again. Check the Manualconnect check box to manually re-establish the connection. Click NEXT to proceed, or BACK to change your settings. Note: Clicking NEXT will not automatically connect the Barricade to the Internet. The Barricade will only connect when you explicitly request it to, for example, by launching your web browser.

4-11 CONFIGURING THE BARRICADE ADSL Settings - PPTP Enter the User ID and Password required by your ISP in the appropriate fields. Enter the Idle Time Out for the Internet connection. @@The default setting is 10 minutes. @@@@You can tell the device to connect manually or automatically as soon as you try to access the Internet again, or to keep the session alive. Click NEXT to proceed, or BACK to change your settings. 4-12 HOME NETWORK SETTINGS Home Network Settings Clicking the Home icon at any time, returns you to this home page. The Main Menu links are used to navigate to other menus that display configuration parameters and statistics. The Barricade's Home Network Settings interface contains four main menu items as described in the following table. Menu Status Description 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. LAN Sets the TCP/IP configuration for the Barricade LAN interface and Settings DHCP clients. WAN Specifies the Internet connection settings. Settings Wireless Configures the radio frequency, SSID, and security for wireless communications. 4-13 CONFIGURING THE BARRICADE Status The Status screen displays WAN/LAN connection status, firmware and hardware version numbers, as well as information on DHCP clients connected to your network. You can also view the Security Log. 4-14 HOME NETWORK SETTINGS The security file, SMCWBR14G2_logfile.log, may be saved by clicking Save and choosing a location. The following items are included on the Status screen: Parameter Current Time INTERNET Renew Home Network (LAN) Description Displays the current time. Displays WAN connection status.

Click on this button to establish a connection to the WAN. Displays system IP settings, as well as DHCP Server, Firewall, UPnP and Wireless status. INFORMATION Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface and for the Barricade, as well as the hardware version and serial number. DHCP Client Log Displays information on DHCP clients on your network. Security Log Save Clear Refresh Displays illegal attempts to access your network.

Click on this button to save the security log file. Click on this button to delete the access log. Click on this button to refresh the screen. 4-15 CONFIGURING THE BARRICADE LAN Settings You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The Barricade must have an IP address for the local network.

The LAN Settings parameters are listed below. Parameter Wireless Router IP Address IP Address IP Subnet Mask DHCP Server DHCP Server DHCP allows individual computers to obtain the TCP/IP configuration at startup from a centralized DHCP server. To dynamically assign an IP address to a client PC, enable the DHCP (Dynamic Host Configuration Protocol) function. The IP address of the Barricade. The IP subnet mask. @@@@@@The domain name is the name you assign to your network. @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@Enter the Idle Time Out for the Internet connection. @@The default setting is 10 minutes. @@@@@@It supports data encryption and client filtering. To use the wireless feature, check the Enable check box and click Save Settings.

After clicking Save Settings, you will be asked to log in again. See "Security" on page 4-27 for details on how to configure wireless security. 4-23 CONFIGURING THE BARRICADE Channel and SSID Enter your wireless network settings on this screen. You must specify a common radio channel and SSID (Service Set ID) to be used by the Barricade and all of its wireless clients. Be sure you configure all of its clients to the same value. For security purposes, you should change the default SSID immediately. Parameter Wireless Network Name (SSID) Broadcast Wireless Network Name Description The Service Set ID (SSID) is the name of your wireless network. The SSID must be the same on the Barricade and all of its wireless clients. (Default: SMC) Enable or disable the broadcasting of the SSID. If you disable broadcast of the SSID, only devices that have the correct SSID can connect.

This nullifies the wireless network "discovery" feature of some products such as Windows XP. (Default: Enable) This device supports the following modes; 11g only, 11b only, and 11b/g mixed mode. (Default: 11b/g mixed mode) Wireless Mode 4-24 HOME NETWORK SETTINGS Parameter Wi-Fi Channel Number Description The radio channel used by the Barricade 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.

(Default: 6) Extend Range Extends the range of the Barricade. (Default: Disable) 4-25 CONFIGURING THE BARRICADE WDS The Wireless Distribution System (WDS) provides a means to extend the range of a Wireless Local Area Network (WLAN).

WDS allows the Barricade to establish a direct link to other wireless base stations and allows clients to roam freely within the area covered by the WDS. To carry out a site survey of available wireless base stations, click Scan. Parameter SSID Description The Service Set ID (SSID) is the name of your wireless network.

The SSID must be the same on the Barricade and all of its wireless clients. This device supports the following modes 11g only, 11b only, and 11b/g mixed mode. The media access control address (MAC address) is a unique identifier attached to each wireless base station. Displays the security mechanism in use. Enables the WDS feature. When enabled, up to 4 WDS links can be set by specifying their Wireless MAC addresses in the MAC address table. Make sure the same channel is in use on all devices. (Default: Disable) Channel MAC Address Security Enable WDS 4-26 SECURITY Security The first menu item in the Security section is Firewall. The Barricade provides a stateful inspection firewall which is designed to protect against Denial of Service (DoS) attacks when activated. Its purpose is to allow a private local area network (LAN) to be securely connected to the Internet.

The second menu item is Wireless. This section allows you to configure wireless security settings according to your environment and the privacy level required. To configure your firewall settings, click Firewall in the left-hand menu. 4-27 CONFIGURING THE BARRICADE Firewall The Barricade'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 "Intrusion Detection" on page 4-35 for details.) The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network.

Enable the firewall feature, and click Save Settings to proceed. 4-28 SECURITY Schedule Rule The first item listed in the Firewall section is Schedule Rule. You may filter Internet access for local clients based on rules. You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time.

First, define the schedule on the Schedule Rule page, then apply the rule on the Access Control page. To add a new rule, click Add Schedule Rule. Proceed to the following page. 4-29 CONFIGURING THE BARRICADE Edit Schedule Rule 1. Define the appropriate settings for a schedule rule (as shown on the following screen).

2. Upon completion, click OK to save your schedule rules, and then click Save Settings to make your settings to take effect. 4-30 SECURITY Access Control Used in conjunction with the Schedule Rule screen, the Access Control screen allows users to define the outgoing traffic permitted or not-permitted. The default is to permit all outgoing traffic. The Barricade can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the Barricade to enter up to 32 MAC addresses that are not allowed access to the WAN port. 1. Click Add PC on the Access Control screen. 2. Define the appropriate settings for client PC services (as shown on the following screen).

3. Click OK and then click Apply to save your settings. The following items are displayed on the Access Control screen: Parameter Enable Filtering Function Normal Filtering Table (up to 10 computers) Description Enables or disables the filtering function. Displays the IP address (or an IP address range) filtering table. 4-31 CONFIGURING THE BARRICADE Access Control Add PC Define the access control list in this page. The settings in the screen shot below will block all email sending and receiving during weekdays (except Friday). See "Schedule Rule" on page 4-29. Define the appropriate settings for client PC services (as shown above). At the bottom of this screen, you can set the scheduling function. You can set this function to Always Blocking or to whatever schedule you have defined in the Schedule Rule screen.

Click OK to save your settings. The added PC will now appear in the Access Control page. For the URL/keyword blocking function, you will need to configure the URL address or blocked keyword on the Parental Control page first. Click Parental Control to add to the list of disallowed URL's and keywords. To enable scheduling, you also need to configure the schedule rule first.

Click Schedule Rule in the left-hand menu to set the times for which you wish to enforce the rule. 4-32 SECURITY MAC Filter Use this page to block access to your network using MAC addresses. The Barricade can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the Barricade to enter up to 32 MAC addresses that are allowed access to the WAN port. All other devices will be denied access.

By default, this feature is disabled. Click Save Settings to proceed, or Cancel to change your settings. 4-33 CONFIGURING THE BARRICADE Parental Control The Barricade allows the user to block access to web sites from a particular PC by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites. You can define up to 30 sites or keywords here. To configure the Parental Control feature, use the table to specify the web sites (www.somesite.com) and/or keywords you want to block on your network. To complete this configuration, you will need to create or modify an access rule in "Access Control Add PC" on page 4-32. To modify an existing rule, click the Edit option next to the rule you want to modify.

To create a new rule, click on the Add PC option. From the Access Control, Add PC section, check the option for WWW with Parental Control in the Client PC Service table to filter out the web sites and keywords selected below, on a specific PC. Click Save Settings to proceed, or Cancel to change your settings. 4-34 SECURITY Intrusion Detection The Barricade's firewall inspects packets at the application layer, maintains TCP and UDP session information including timeouts and number of active sessions, and provides the ability to detect and prevent certain types of network attacks such as Denial-of-Service (DoS) attacks. 4-35 CONFIGURING THE BARRICADE Network attacks that deny access to a network device are called 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 DoS attacks including: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Brute-force attack, Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attack), UDP port loopback, Snork Attack. Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network. 4-36 SECURITY The table below lists the Intrusion Detection parameters and their descriptions.

Parameter Intrusion Detection Feature SPI and Anti-DoS No firewall protection The Intrusion Detection feature of the Barricade limits the access of incoming traffic at the WAN port. When the Stateful Packet Inspection (SPI) feature is turned on, all incoming packets are blocked except those types marked with a check in the SPI section at the top of the screen. Defaults Description RIP Defect Disabled If the router does not reply to an IPX RIP request packet, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets accumulating.

Don't discard Prevents a ping on the router's WAN port from being routed to the network. Discard Ping to WAN 4-37 CONFIGURING THE BARRICADE Parameter Stateful Packet Inspection Defaults Description Enabled This option allows you to select different application types that are using dynamic port numbers. If you wish to use Stateful Packet Inspection (SPI) for blocking packets, click on the Yes radio button in the "Enable SPI and Anti-DoS firewall protection" field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service and TFTP Service. It is called a "stateful" packet inspection because it examines the contents of the packet to determine the state of the communication; i.e.

, it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until a connection to the specific port is requested. When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks FTP Service in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN. When hackers attempt to enter your network, we can alert you by email Your E-mail Address SMTP Server Address POP3 Server Address User Name Enter your email address. Enter your SMTP server address (usually the part of the email address following the "@" sign). Enter your POP3 server address (usually the part of the email address following the "@" sign). Enter your email account user name. 4-38 SECURITY Parameter Password Connection Policy Fragmentation half-open wait 10 secs Configures the number of seconds that a packet state structure remains active.

When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. Defines how long the software will wait for a TCP session to reach an established state before dropping the session. Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. Defaults Description Enter your email account password. TCP SYN wait 30 secs TCP FIN wait TCP connection idle timeout 5 secs 3600 secs The length of time for which a TCP session will be (1 hour) managed if there is no activity. The length of time for which a UDP session will be managed if there is no activity. Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions. Defines the rate of new unestablished sessions that will cause the software to stop deleting half-open sessions. Maximum number of allowed incomplete TCP/UDP sessions per minute. Minimum number of allowed incomplete TCP/UDP sessions per minute.

Maximum number of incomplete TCP/UDP sessions from the same host. UDP session idle 30 secs timeout DoS Detect Criteria Total incomplete TCP/UDP sessions HIGH Total incomplete TCP/UDP sessions LOW 300 sessions 250 sessions Incomplete 250 TCP/UDP sessions sessions (per min.) HIGH Incomplete 200 TCP/UDP sessions sessions (per min.) LOW Maximum incomplete TCP/UDP sessions number from same host 10 sessions 4-39 CONFIGURING THE BARRICADE Parameter Incomplete TCP/UDP sessions detect sensitive time period Maximum half-open fragmentation packet number from same host Half-open fragmentation detect sensitive time period Flooding cracker block time Defaults Description 300 msecs Length of time before an incomplete TCP/UDP session is detected as incomplete. 30 sessions Maximum number of half-open fragmentation packets from the same host.

1 sec Length of time before a half-open fragmentation session is detected as half-open. Length of time from detecting a flood attack to blocking the attack. 300 secs Note: We do not recommend modifying the default parameters shown above. Click Save Settings to proceed, or Cancel to change your settings. 4-40 SECURITY DMZ If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access.

Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort. 4-41 CONFIGURING THE BARRICADE Wireless The Barricade can be quickly configured for roaming clients by setting the Service Set Identifier (SSID) and channel number. It supports data encryption and client filtering. To use the wireless feature, check the Enable check box and click Save Settings. To begin configuring your wireless security settings, click Wireless Encryption. 4-42 SECURITY Wireless Encryption The Barricade can transmit your data securely over a wireless network. Matching security mechanisms must be set up on your Barricade and your wireless client devices. Select the most suitable security mechanism from the drop-down list on this screen. Parameter No WEP, No WPA/WPA2 Description Disables all wireless security.

To make it easier to set up your wireless network, we recommend enabling this setting initially. By default, wireless security is disabled. Once you have your wireless network in place, the minimum security we recommend is to enable the legacy security standard, Wired Equivalent Privacy (WEP).