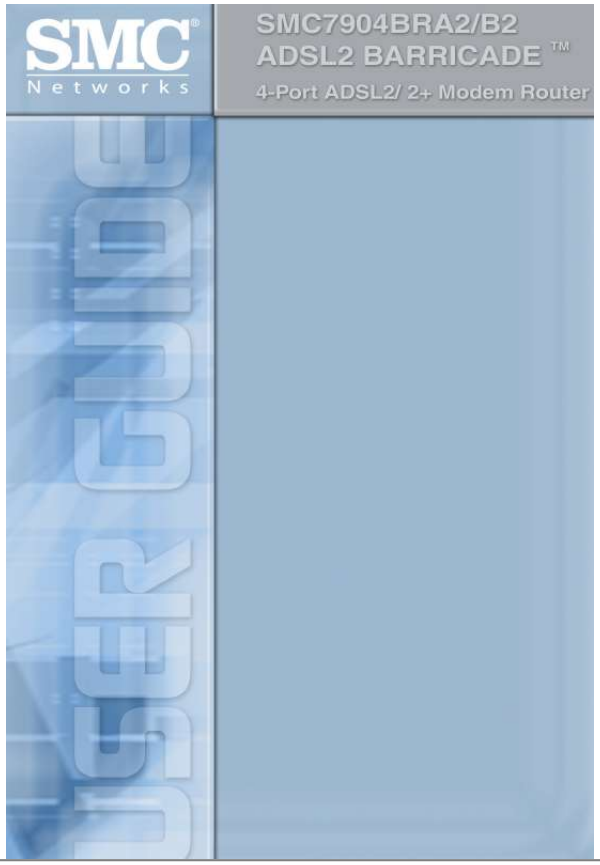

Manual abstract:

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: any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. iii COMPLIANCES EC Conformance Declaration SMC contact for these products in Europe is: SMC Networks Europe, Edificio Conata II, Calle Fructuós Gelabert 6-8, 2o, 4a, 08970 - Sant Joan Despí, 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 55022 EN 55024 EN 61000-3-2 EN 61000-3-3 EN 60950-1 iv 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. Verwenden Sie keine Flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung. 4. Die Netzanschlu ßsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein. 5.

Das Gerät ist vor Feuchtigkeit zu schützen. 6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen. 7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden. 8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte. 9.
Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden. 10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten. 11.
Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden. 12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw.
elektrischen Schlag auslösen. 13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden. 14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen: a. b. c. d. Netzkabel oder Netzstecker sind beschädigt.

Flüssigkeit ist in das Gerät eingedrungen. Das Gerät war Feuchtigkeit ausgesetzt. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen. e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt. f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist. 15. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden. Für einen Nennstrom bis 6 A und einem Gerätegewicht größer 3 kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.
75 mm2 einzusetzen. Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70 dB(A) oder weniger. v COMPLIANCES vi TABLE OF CONTENTS Introduction . . .

. . . . .
. . . . .
Disable HTTP Proxy . . . . . .

. . . . . .
. . . . .
. . . . .
. . . . Obtain IP Settings from Your Barricade . . . . . .

. . . . . .
. . . Windows XP . .
. . . . .
. . . . . .

. . . . . .
. . . . .
. . . . .
. . . . . .

Disable HTTP Proxy . . . . . .
. . . . .
. . . . .
. . . . . .

. . . . Obtain IP Settings from Your Barricade . . . . . .
. . . . .
. . . . .
. . . Configuring Your Macintosh Computea 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. It is simple to configure and can be up and running in minutes. Features and Benefits · · · · · Intergrated ADSL modem for connecting to ADSL line Local network connection via four 10/100 Mbps Ethernet ports DHCP for dynamic IP configuration, and DNS Proxy/Relay for domain name mapping 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 1-1 INTRODUCTION 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: · Wired LAN The Barricade provides connectivity to 10/100 Mbps 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.

· Shared IP Address Using only one ISP account, multiple users on your network can access the Internet at the same time. 1-2 APPLICATIONS · 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. · 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.

1-3 INTRODUCTION · 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 BarricadeTM, 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 BarricadeTM on page 4-1. Package Contents After unpacking, check the contents of the box to be sure you have received the following components: · · · · · · · ADSL2 BarricadeTM (SMC7904BRA2 or SMC7904BRB2) Power adapter One CAT-5 Ethernet cable (RJ-45) One Telephone patch cables (RJ-11) Documentation CD One Warranty Card One Splitter for NE (the Netherlands), UK and FR (France) versions only 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 Internet Service installed. Ethernet Adapter installed on each PC. TCP/IP network protocols installed on each PC that will access the Internet. A Java enabled web browser such as Internet Explorer 5.

5 or above, Netscape 4.7 or above, Mozilla 1.7 or above and Firefox 1.0 or above. Hardware Description The Barricade contains an integrated ADSL2+ modem and connects to the Internet or to a remote site using its WAN port. This device 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 1 Mbps upstream. G.lite (or splitterless) ADSL provides up to 1.

5 Mbps downstream and 512 kbps upstream. ADSL2+ Provides up to 24 Mbps downstream and 1 Mbps 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. 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 SMC7904BRA2 contains the following ports on the rear panel: 12 1A Figure 2-1. SMC7904BRA2 Rear Panel Item ADSL Port LAN1 to LAN4 Reset Button Description Connect your ADSL line to this port (RJ-11 port). 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 Barricade and restore the default factory settings. To reset without losing configuration settings, see "Reset" on page 4-70. Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may damage the Barricade. Power Inlet 2-3 INSTALLATION SMC7904BRB2 contains the following ports on the rear panel: 12 1A Figure 2-2. SMC7904BRB2 Rear Panel Item ADSL Port LAN1 to LAN4 Reset Button Description Connect your ADSL line to this port (RJ-45 port). 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 Barricade and restore the default factory settings. To reset without losing configuration settings, see "Reset" on page 4-70. Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may damage the Barricade. Power Inlet 2-4 HARDWARE DESCRIPTION LED Indicators (SMC7904BRA2) The power and port LED indicators on the front panel for SMC7904BRA2 are illustrated in the following figure and table. 4-port Annex A ADSL2/2+ Modem Router SMC7904BRA2 Figure 2-3. SMC7904BRA2 Front Panel LED Power Status On Off LAN (4 LEDs) On Flashing Off ADSL Sync On Flashing Off ADSL Data Blinking Off Description The Barricade is receiving power. Normal operation. Power off or failure.

Ethernet connection is established. The indicated LAN port is sending or receiving data. There is no LAN connection on the port. ADSL connection is functioning correctly. The Barricade is establishing an ADSL link.

ADSL connection is not established. ADSL port is sending/receiving data. No data is being transferred. 2-5 INSTALLATION LED Indicators (SMC7904BRB2) The power and port LED indicators on the front panel for SMC7904BRB2 are illustrated in the following figure and table. Figure 2-4. SMC7904BRB2 Front Panel LED Power Status On Off LAN (4 LEDs) On Flashing Off ADSL Sync On Flashing Off ADSL Data Blinking Off Description The Barricade is receiving power. Normal operation. Power off or failure. Ethernet connection is established. The indicated LAN port is sending or receiving data. There is no LAN connection on the port. ADSL connection is functioning correctly. The Barricade is establishing an ADSL link. ADSL connection is not established. ADSL port is sending/receiving data.

No data is being transferred. 2-6 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 ADSL cable from the port labelled ADSL on the Splitter/Microfilter to the ADSL port on your Barricade. When inserting the plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. Note: The ADSL port of SMC7904BRA2 is RJ-11. The ADSL port of SMC7904BRB2 is RJ-45.

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 or 100 Mbps, 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. Note: Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. Category 5 cable is recommended. 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 CONNECT THE SYSTEM Connection Illustration The connection diagram shows how to connect the Barricade. 2-9 INSTALLATION 2-10 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 2000" on page 3-2 "Windows XP" on page 3-5 "Configuring Your Macintosh Computer" on page 3-7 depending on your operating system. 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 BarricadeTM" on page 4-1 for instruction on configuring the Barricade.) 3-1 CONFIGURING CLIENT PC 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. 3-2 WINDOWS 2000 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. See page 3-5 for details.

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. 3-3 CONFIGURING CLIENT PC 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. Close the Command Prompt window. Your computer is now configured to connect to the Barricade. 3-4 WINDOWS XP 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 the options. 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. Follow these steps to disable the HTTP proxy: Open your web browser, go to Tools/Internet Options, select the Connections tab, click LAN Setting. Make sure the checkbox for Use a proxy server for your LAN is not checked.

3-5 CONFIGURING 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. 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.

Close the Command Prompt window. Your computer is now configured to connect to the Barricade. 3-6 CONFIGURING YOUR MACINTOSH COMPUTER 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. 3-7 CONFIGURING CLIENT PC 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 Explorer/ Preferences. 2. In the Internet Explorer Preferences window, under Network, select Proxies. 3-8 CONFIGURING YOUR MACINTOSH COMPUTER 3.

Uncheck all check boxes and click OK. 3-9 CONFIGURING CLIENT PC 3-10 CHAPTER 4 CONFIGURING THE BARRICADETM After you have configured TCP/IP on a client computer, you can configure the Barricade using your web browser. 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. Note: Password is case sensitive. This is the login screen for SMC7904BRA2: This is the login screen for SMC7904BRB2: 4-1 CONFIGURING THE BARRICADETM Navigating the Management Interface The first screen of the web management is the Status screen. You can view the device status summary here.
The Barricade's management interface consists of a Setup Wizard and 13 menu items. Use the Setup Wizard to quickly set up the Barricade. Go to "SETUP WIZARD" on page 4-4 for details. For configuration details of the 13 menu items, please refer to "Configuration parameters" on page 4-16. 4-2 NAVIGATING THE MANAGEMENT INTERFACE Making Configuration Changes Configurable parameters have a dialog box or a drop-down menu. Once a configuration change has been made on a screen, click the APPLY or SAVE SETTINGS or NEXT button at the bottom of the screen 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 BARRICADETM SETUP WIZARD Time Zone Click on SETUP WIZARD and NEXT, you will see the time zone screen. Select your local time zone from the drop down menu.
This information is used for log entries and client filtering. @@Select the desired servers from the drop down menu. Click NEXT to continue. 4-4 SETUP WIZARD 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 ISP uses Protocols PPPoA or PPPoE you will need to enter the username and password supplied by your ISP. If your ISP uses Protocol RFC1483 Routed you will need to enter the IP address, Subnet Mask, and Default Gateway supplied by your ISP. If your Country or Internet Service Provider is not listed in this screen, you will need to manually enter settings. Go to "Parameter Setting Country or ISP Not Listed" on page 4-6 in the manual. Note: If your ISP has not provided you with a DNS address and the protocol is PPPoA, PPPoE or 1483 Bridging, you can leave this field blank.

The Barricade will then automatically obtain the DNS address. Click NEXT to continue. 4-5 CONFIGURING THE BARRICADETM Parameter Setting - Country or ISP Not Listed If your Country or Internet Service Provider is not listed, select Other. This will allow you to manually configure your ISP settings. For manual configuration you will need to know the Protocol, DNS Server, Encapsulation and VPI/VCI settings used by your ISP. If you have a static IP address you will also need to know the IP address, Subnet Mask and Gateway address. Please contact your ISP for these details if you do not already have them. After selecting Other, then select the Protocol that your ISP uses from the drop down menu. 4-6 SETUP WIZARD PPPoE Parameter VPI/VCI Encapsulation Username Password Confirm Password Description @@Select the encapsulation used by ISP from the drop down menu. Enter user name provided by your ISP.
Enter password provided by your ISP. Confirm password Click NEXT to continue to the "Confirm" settings screen. Go to "Confirm" on page 4-14 in the manual for details about the settings. 4-7 CONFIGURING THE BARRICADETM PPPoA Parameter VPI/VCI Encapsulation Username Password Confirm Password Description @@Select the encapsulation used by ISP from the drop down list. Enter user name provided by your ISP.
Enter password provided by your ISP. Confirm password Click NEXT to continue to the "Confirm" settings screen. Go to "Confirm" on page 4-14 in the manual for details about the settings. 4-8 SETUP WIZARD 1483 Bridging (DHCP) Parameter DNS Server Description Enter the DNS Server IP address provided by your ISP. If your ISP has not provided you with a DNS address, leave this field blank.
The Barricade will automatically obtain the DNS address from your ISP. @@Select the encapsulation used by ISP from the drop down menu. VPI/VCI Encapsulation Click NEXT to continue to the "Confirm" settings screen. Go to "Confirm" on page 4-14 in the manual for details about the setting. 4-9 CONFIGURING THE BARRICADETM 1483 Bridging (Static) Parameter IP Address Subnet Mask Default Gateway DNS Server VPI/VCI Encapsulation Description Enter your ISP supplied static IP address here Enter the subnet mask address provided by your ISP. Enter the gateway address provided by your ISP. Enter the DNS Server IP address provided by your ISP. @@Select the encapsulation used by ISP from the drop down list. Click NEXT to continue to the "Confirm" settings screen. Go to "Confirm" on page 4-14 in the manual for details about the settings.

4-10 SETUP WIZARD 1483 Routing Parameter IP Address Subnet Mask Default Gateway DNS Server VPI/VCI Encapsulation Description Enter the IP address provided by your ISP. Enter the subnet mask address provided by your ISP. Enter the gateway address provided by your ISP. Enter the DNS Server IP address provided by your ISP. @@@@Go to "Confirm" on page 4-14 in the manual for details about the settings. 4-11 CONFIGURING THE BARRICADETM Bridging Parameter Management IP Address Description Management IP address of the Barricade (Default:192.168.2.1). When configured in "Bridging" mode you will be able to manage the Barricade using this IP address.

@@Select the encapsulation used by ISP from the drop down menu. VPI/VCI Encapsulation Click NEXT to continue to the "Confirm" settings screen. Go to "Confirm" on page 4-14 in the manual for details about the settings. 4-12 SETUP WIZARD 1483 Routing (DHCP) Parameter DNS Server VPI/VCI Encapsulation Description Enter the DNS Server IP address provided by your ISP. @@@@@@@@The WAN protocol of your ISP. @@Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). @@@@Go to page 4-21 for a detailed description. @@WAN subnet mask (only displayed if you have static IP). @@@@The ISP assigned user name. @@Your Barricade is now set up. @@Configures the Internet connection settings. @@Configures Address Mapping, virtual server and special applications. Sets the routing parameters and displays the current routing table. @@Community string and trap server settings. Enable/disable the Universal Plug and Play function. Allows you to optimize your network traffic. @@@@@@@@@@@@Select your time zone from the drop down menu. @@@@Select the desired servers from the drop down menu. 4-18 CONFIGURATION PARAMETERS Password Settings Use this screen to change the password for accessing the management interface. 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 10 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) 4-19 CONFIGURING THE BARRICADETM 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 Save Settings. 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, 211.20.16.

1:8080. 4-20 CONFIGURATION PARAMETERS WAN Specify the WAN connection parameters provided by your Internet Service Provider (ISP). The following three items are configurable: · · · ATM PVC Clone MAC DNS 4-21 CONFIGURING THE BARRICADETM ATM PVC To configure your Internet Connection settings, select ATM PVC, then VC1. Click the VC to set the detailed parameters. Note: The Barricade can support up to 8 Virtual Circuits (VC's). Multiple VC's, in general, are only used in the case of Triple Play (Internet/Voice/Video) services. Example: VC1 = Internet, VC2 = Voice, VC3 = Video. Unless stated by your ISP, you will use a single VC. In this case "VC1"should be used. Parameter VC1 to VC8 VPI/VCI Encapsulation Description Click on the desired VC to configure the connection parameters. Displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) configured for the corresponding VC. Displays the Encapsulation configured for the corresponding VC. Encapsulation 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).

· Protocol Displays the Protocol configured for the corresponding VC. 4-22 CONFIGURATION PARAMETERS ATM Interface 1483 Bridging Enter the settings provided by your ISP. In Bridging mode the Barricade will act as a bridge passing the IP addressing directly to the attached client PC. Parameter VLAN Description Select VLAN group from the drop-down menu. New VLAN groups can be created from the LAN menu. @@Select the encapsulation used by ISP from the drop-down menu. ATM QoS classes including CBR, UBR and VBR QoS Parameters - PCR (Peak Cell Rate), SCR (Sustainable Cell Rate) and MBS (Maximum Burst Size) are configurable. VPI/VCI Encapsulation QoS Class PCR/SCR/MBS 4-23 CONFIGURING THE BARRICADETM PPPoA Parameter VPI/VCI Encapsulation QoS Class PCR/SCR/MBS IP assigned by ISP IP Address Subnet Mask Connect Type Description @@Select the encapsulation used by ISP from the drop-down menu. ATM QoS classes including CBR, UBR and VBR QoS Parameters - PCR, SCR and MBS are configurable. Select Yes if the IP address was provided by your ISP Enter the IP address provided by your ISP.

For dynamic IP leave this field blank. Enter the subnet mask address provided by your ISP. For dynamic IP leave this field blank. Sets connection mode to Always connected, Auto-Triggered by traffic or Manual connection. For flat rate services use Always connected.

Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. This setting only applies when the Connect Type is set to Auto-Triggered by traffic. Enter user name. Enter password.

Idle Time (Minute) Username Password 4-24 CONFIGURATION PARAMETERS Parameter Confirm Password MTU Description Confirm password Leave the Maximum Transmission Unit (MTU) at the default value unless instructed by your ISP 1483 Routing Parameter IP Address Subnet Mask Default Gateway VPI/VCI Encapsulation QoS Class PCR/SCR/MBS DHCP Client Description Enter the IP address provided by your ISP. Enter the subnet mask address provided by your ISP. Enter the gateway address provided by your ISP. @@Select the encapsulation used by ISP from the drop down list. ATM QoS classes including CBR, UBR and VBR QoS Parameters - PCR, SCR and MBS are configurable. Check the box if your ISP assigns an IP address dynamically. 4-25 CONFIGURING THE BARRICADETM PPPoE Parameter VPI/VCI Encapsulation QoS Class PCR/SCR/MBS IP assigned by ISP IP Address Subnet Mask Connect Type Description @@Select the encapsulation used by ISP from the drop-down menu. ATM QoS classes including CBR, UBR and VBR QoS Parameters - PCR, SCR and MBS are configurable. Select yes, if your ISP assigns IP address dynamically. If you have selected "No" in the previous field, type in the IP address provided by your ISP.

Enter the subnet mask address provided by your ISP. Sets connection mode to Always connected, Auto-Triggered by traffic or Manual connection. For flat rate services use Always connected. Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated.

This setting only applies when the Connect Type is set to Auto-Triggered by traffic. Enter user name. Enter password. Idle Time (Minute) Username Password 4-26 CONFIGURATION PARAMETERS Parameter Confirm Password MTU Description Confirm password Leave the Maximum Transmission Unit (MTU) at the default value unless instructed by your ISP. IP Over RFC1483 bridged Parameter IP Address Subnet Mask Default Gateway VPI/VCI Encapsulation QoS Class PCR/SCR/MBS DHCP Client Description Enter the IP address provided by your ISP.

Enter the subnet mask address provided by your ISP. Enter the gateway address provided by your ISP. @@Select the encapsulation used by ISP from the drop-down menu. ATM QoS classes including CBR, UBR and VBR QoS Parameters - PCR, SCR and MBS are configurable. Check the box if your ISP assigns an IP address dynamically.

4-27 CONFIGURING THE BARRICADETM Clone MAC Address Some ISPs require you to register your MAC address with them. If this is the case, and you have previously registered the MAC address of another device, the MAC address of the Barricade must be changed to the MAC address that you have registered with your ISP. 4-28 CONFIGURATION PARAMETERS DNS A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.

com, a DNS server will find that name in its index and find the matching IP address: xxx.xxx.xxx.xxx. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here. 4-29 CONFIGURING THE BARRICADETM LAN The LAN settings menu allows you to change the default IP address of the Barricade, modify the DHCP server settings and create VLAN's. Parameter LAN IP IP Address IP Subnet Mask DHCP Server VLAN Binding LAN1 to LAN4 Description The IP address of the Barricade. The subnet mask of the Barricade.

This option allows you to enable or disable the DHCP server function. By default DHCP is enabled. This option allows you to change VLAN membership of LAN ports 1-4. By default all LAN ports are assigned to the "default" VLAN. Allows you to define a name for the DHCP server. DHCP Server DHCP Server ID 4-30 CONFIGURATION PARAMETERS Parameter Lease Time Description Allows you to select a pre-defined lease time for IP addresses assigned using DHCP. For home networks this may be set to Forever, which means there is no time limit on the IP address lease. 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.

Specify the end IP address of the DHCP pool. If your network uses a domain name, enter it here. Otherwise, leave this field blank. IP Address Pool Start IP Address End IP Address Domain Name VLAN The Barricade's VLAN function can be used to create up to 4 VLAN profiles. Once a VLAN profile is created interfaces can be assigned to the VLAN profile.

This is done by setting the VLAN binding. Notes: Only interfaces of IEEE 802 bridging type (LAN ports 1-4 and 1483 Bridging PVC's) can be assigned to a VLAN. Click Add VLAN to create a profile. 4-31 CONFIGURING THE BARRICADETM VLAN Profile Configure the VLAN settings in this screen. · · · · · Description: Enter a description for the VLAN group, for example: Admin PC's IP Address: Enter IP address for the VLAN. Subnet Mask: Enter Subnet Mask address for the VLAN. NAT Domain: Set NAT Domain to private or public. IGMP Snooping: IGMP Snooping: Internet Group Management Protocol (IGMP) snooping is a method by which Layer 2 devices can "listen in" on IGMP conversations between hosts and routers. When a switch hears a group join message from a host, it notes which switch interface it heard the message on, and adds that interface to the group. Similarly, when a Layer 2 switch hears a group leave message or a response timer expires, the switch will remove that host's switch interface from the group.

IGMP Querier: IGMP Querier: if the IGMP Querier is enabled, then the router will periodically query all multicast group members on the specified VLAN. · 4-32 CONFIGURATION PARAMETERS NAT Network Address Translation (NAT) allows multiple users to access the Internet sharing one public IP. 4-33 CONFIGURING THE BARRICADETM 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. 4-34 CONFIGURATION PARAMETERS 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.

4-35 CONFIGURING THE BARRICADETM 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 screens to specify the additional public ports to be opened for each application. 4-36 CONFIGURATION PARAMETERS NAT Mapping Table This screen displays the current NAPT (Network Address Port Translation) address mappings. Click Refresh to update the table. 4-37 CONFIGURING THE BARRICADETM ROUTING These screens define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters. 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. 4-38 CONFIGURATION PARAMETERS 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 Sets the RIP (Routing Information Protocol) version to use on this interface. 4-39 CONFIGURING THE BARRICADETM Parameter Poison Reverse Authentication Required Description A method for preventing loops that would cause endless retransmission of data traffic. · · 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. 4-40 CONFIGURATION PARAMETERS Routing Table Parameter Description Flags 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. 4-41 CONFIGURING THE BARRICADETM 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-of-Service (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. (For details see page 4-49.) The firewall does not significantly affect system performance, so we advise enabling the function to protect your network.
Select Enable and click the SAVE SETTINGS button. 4-42 CONFIGURATION PARAMETERS Access Control Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic. The following items are on the Access Control screen: Parameter Enable Filtering Function Description Enable or Disable Access control function. Normal Filtering Table Displays descriptive list of filtering rules defined.
4-43 CONFIGURING THE BARRICADETM To create a new access control rule: 1. Click Add PC on the Access Control screen. The Access Control Add PC screen will appear. 2. Define the appropriate settings for client PC services.
3. Click OK and then click SAVE SETTINGS to save your settings. 4-44 CONFIGURATION PARAMETERS MAC Filter The MAC Filter allows you to define what client PC's can access the Internet. When enabled only the MAC addresses defined in the MAC Filtering table will have access to the Internet. All other client devices will be denied access. You can enter up to 32 MAC addresses in this table. · · MAC Address Control: select enable or disable. MAC Filtering Table: enter the MAC address in the space provided. 4-45 CONFIGURING THE BARRICADETM URL Blocking The Barricade allows the user to block access to web sites 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 here. 4-46 CONFIGURATION PARAMETERS Schedule Rule You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the schedule on the Schedule Rule screen, and apply the rule on the Access Control screen. 4-47 CONFIGURING THE BARRICADETM Follow these steps to add a schedule rule: 1. Click Add Schedule Rule on the Schedule Rule screen. The Edit Schedule Rule screen will appear. 2. Define the appropriate settings for a schedule rule. 3.
Click OK and then click SAVE SETTINGS to save your settings. 4-48 CONFIGURATION PARAMETERS Intrusion Detection · Intrusion Detection Feature Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: Enabled) -- The Intrusion Detection Feature of the Barricade Router limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked in the Stateful Packet Inspection section. RIP Defect (Default: Enabled) -- If an RIP request packet is not acknowledged to by the router, 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 from accumulating. Discard Ping to WAN (Default: Disabled) -- Prevent a ping on the Barricade's WAN port from being routed to the network. Scroll down to view more information. 4-49 CONFIGURING THE BARRICADETM 4-50 CONFIGURATION PARAMETERS · Stateful Packet Inspection This is called a "stateful" packet inspection because it examines the contents of the packet to determine the state of the communications; 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 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. Stateful Packet Inspection allows you to select different application types that are using dynamic port numbers. If you wish to use the Stateful Packet Inspection (SPI) to block 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, H.323 Service, or TFTP Service. · When hackers attempt to enter your network, we can alert you by e-mail Enter your email address. Specify your SMTP and POP3 servers, user name, and password.

4-51 CONFIGURING THE BARRICADETM · Connection Policy Enter the appropriate values for TCP/UDP sessions as described in the following table. Parameter Fragmentation half-open wait Defaults Description 10 sec 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 synchronize before dropping the session. Specifies how long a TCP session will be maintained after the firewall detects a FIN packet. The length of time for which a TCP session will be managed if there is no activity. The length of time for which a UDP session will be managed if there is no activity. The length of time for which an H.323 session will be managed if there is no activity. TCP SYN wait 30 sec TCP FIN wait 5 sec TCP connection idle timeout UDP session idle timeout 3600 seconds (1 hour) 30 sec H.

323 data channel 180 sec idle timeout 4-52 CONFIGURATION PARAMETERS · DoS Criteria and Port Scan Criteria Set up DoS and port scan criteria in the spaces provided (as shown below). Parameter Total incomplete TCP/UDP sessions HIGH Total incomplete TCP/UDP sessions LOW Incomplete TCP/UDP sessions (per min) HIGH Incomplete TCP/UDP sessions (per min) LOW Defaults Description 300 sessions 250 sessions 250 sessions 200 sessions 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 halfopen 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. Maximum incomplete 10 TCP/UDP sessions number from same host Incomplete TCP/UDP sessions detect sensitive time period 300 msec Length of time before an incomplete TCP/UDP session is detected as incomplete. Maximum half-open 30 fragmentation packet number from same host 10000 Half-open fragmentation detect msec sensitive time period Flooding cracker block time 300 second Maximum number of half-open fragmentation packets from the same host. 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.

Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network. 4-53 CONFIGURING THE BARRICADETM 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. 4-54 CONFIGURATION PARAMETERS SNMP Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). Select the SNMP Operation mode from the drop down menu. 4-55 CONFIGURING THE BARRICADETM Community A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the Barricade, the NMS must first submit a valid community string for authentication. Parameter Community Access Valid Description A community name authorized for management access.

Management access is restricted to Read Only (Read) or Read/Write (Write). Enables/disables the entry. Note: Up to five community names may be entered. 4-56 CONFIGURATION PARAMETERS Trap Specify the IP address of the NMS to notify when a significant event is detected by the agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMS specified as a trap receiver. Parameter Description IP Address Traps are sent to this address when errors or specific events occur on the network. Community A community string (password) specified for trap management. Enter a word, something other than public or private, to prevent unauthorized individuals from accessing information on your system. Version Sets the trap status to disabled, or enabled with V1 or V2c. The v2c protocol was proposed in late 1995 and includes enhancements to v1 that are universally accepted.

These include a get-bulk command to reduce network management traffic when retrieving a sequence of MIB variables, and a more elaborate set of error codes for improved reporting to a Network Management Station. 4-57 CONFIGURING THE BARRICADETM UPNP The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the office, home and everywhere within your network.